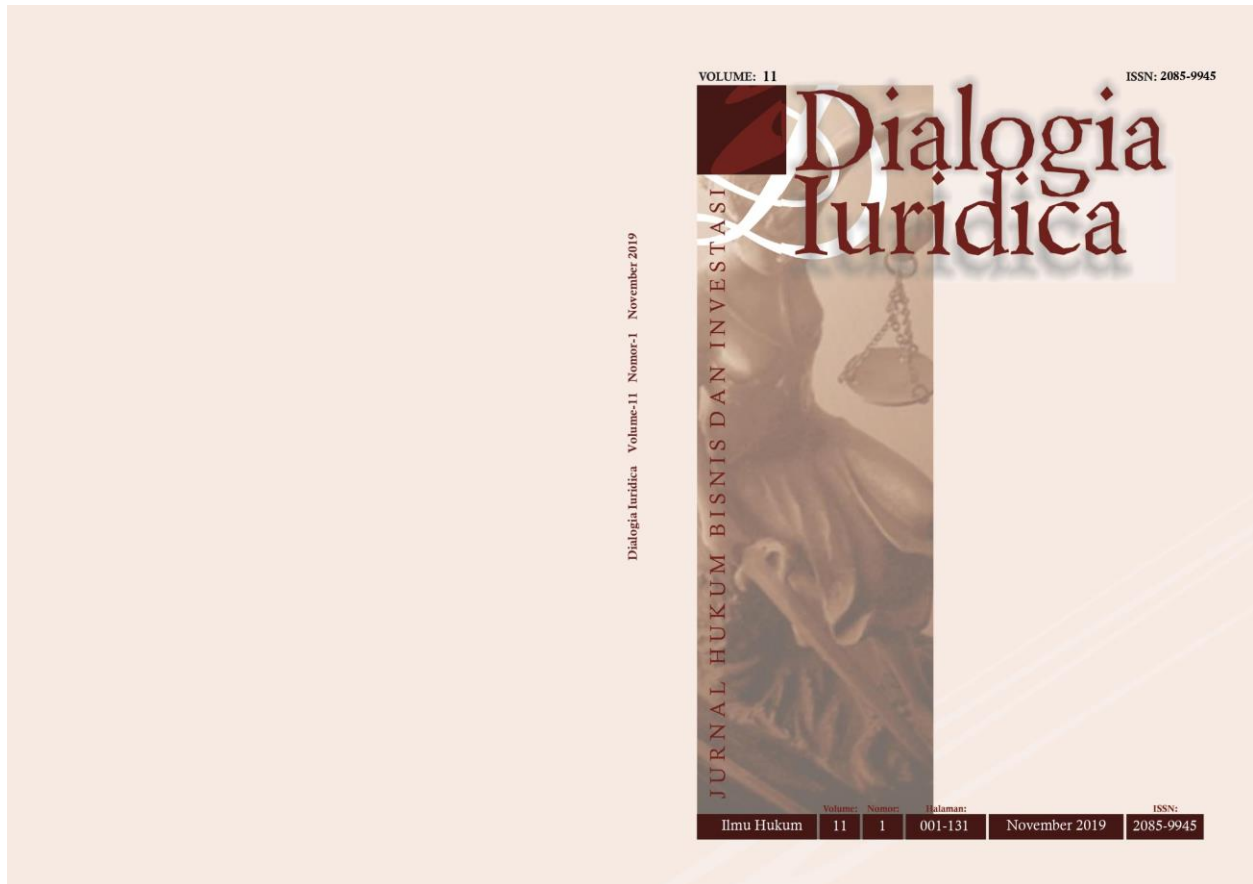


1. [Home](#) /
2. [Archives](#) /
3. Vol. 11 No. 1 (2019): Volume 11 Nomor 1 Tahun 2019

Vol. 11 No. 1 (2019): Volume 11 Nomor 1 Tahun 2019



Published: 2019-11-19

Articles

- [MEWUJUDKAN PENEGAKAN HUKUM YANG BAIK DI NEGARA HUKUM INDONESIA](#)

Laurensius Arliman. S, Scopus ID: 57202

1-20

◦ [PDF](#)

- [KEWENANGAN UNITED NATIONS COMMITTEE ON THE PEACEFUL USES OF OUTER SPACE \(UNCOPUOS\) DALAM PEMBENTUKAN HUKUM ANTARIKSA INTERNASIONAL](#)

Diogenes Diogenes

21-42

◦ [PDF](#)

- [AMBIGUITAS PENGATURAN KEADAAN BAHAYA DALAM SISTEM KETATANEGARAAN INDONESIA](#)

Agus Adhari

43-61

◦ [PDF](#)

- [PERLINDUNGAN PERLINDUNGAN HUKUM BAGI KONSUMEN TERHADAP IKLAN TELEVISI YANG BERMUATAN MATERI PORNOGRAFI MELALUI CLASS ACTION](#)

Radhyca Nanda

62-76

◦ [PDF](#)

- [PROBLEMATIKA PENGATURAN CYBERSTALKING \(PENGUNTITAN DI DUNIA MAYA\) DENGAN MENGGUNAKAN ANONYMOUS ACCOUNT PADA SOSIAL MEDIA](#)

Rahel Octora

77-96

◦ [PDF](#)

- **PERBANDINGAN PENYELESAIAN SENGKETA MEREK BERDASARKAN UNDANG-UNDANG MEREK NOMOR 20 TAHUN 2016 TENTANG MEREK DAN INDIKASI GEOGRAFIS JO. UNDANG-UNDANG NOMOR 30 TAHUN 1999 TENTANG ARBITRASE DAN ALTERNATIF PENYELESAIAN SENGKETA DENGAN WORLD INTELLECTUAL PROPER**

Shelly Kurniawan

97-113

- [PDF](#)
- **DISKRIMINASI HUKUM DALAM PEMBERANTASAN KORUPSI POLITIK DI DAERAH**

Jupri Jupri, Roy Marthen Moonti

114-131

- [PDF](#)

**PROBLEMATIKA PENGATURAN *CYBERSTALKING* (PENGUNTITAN DI DUNIA
MAYA) DENGAN MENGGUNAKAN *ANONYMOUS ACCOUNT* PADA SOSIAL
MEDIA**

Rahel Octora

Fakultas Hukum, Universitas Kristen Maranatha

octorael@hotmail.com

Submitted: 2019-09-18 | Reviewed: 2019-10-31 | Accepted: 2019-11-07

Abstract

Technology develops, patterns of interaction between people also change. The internet is a new world where humans interact, without limitation of distance and time. In the real world, as legal subjects, everyone must have a clear identity, proof of identification, so that the state can recognize it and the law can be upheld against it, as well as the law can protect their rights. Social media which is currently developing, allows everyone to appear and interact in cyberspace either by showing their true identity, or by using fake identities, or even interacting without identity (anonymous). Easily each person can create more than one e-mail account, which can be used to create more than one social media account. Although the creation of e-mail and social media accounts is through the cell phone number verification stage, this does not solve the problem because anyone can easily have multiple cellphone numbers. A person in cyber world can be an anonymous subject and take various actions that harm others, including stalking others. Stalking, done by the person behind an anonymous account is an annoying action, has not been regulated clearly in Indonesian. This paper is the result of a normative juridical study. Result of this research is: criminal law regulation system in Indonesia regulated cyberstalking as long as the action consist of delivery of illegal contents such as threats, obscene content and insults. Further regulation is still needed, especially regarding law enforcement mechanisms for perpetrators that are difficult to reach due to the use of the anonymous account.

Keywords: *Anonymous account; cyberstalking; regulation.*

PENDAHULUAN

Manusia sebagai bagian dari masyarakat senantiasa membutuhkan interaksi dengan sesamanya. Interaksi yang semula berlangsung secara tatap muka semakin bergeser seiring dengan perkembangan teknologi. Internet dengan mudah menjadi sarana yang menghubungkan orang

dengan orang. Orang dapat berinteraksi tanpa terbatas jarak dan waktu. Dunia *cyber* adalah dunia virtual, di mana setiap orang dapat membangun citra dirinya melalui identitas yang dibuat dan kemudian ditampilkan. Identitas yang muncul di dunia maya mungkin saja bukan identitas asli dari orang yang bersangkutan. Orang dapat berpura-pura menjadi orang lain atau bahkan dirinya dapat berkhayal menjadi siapapun, dan kemudian berinteraksi dengan orang lain melalui perantaraan sosial media. Sosial media merupakan media online di mana penggunanya dapat berbagi, berpartisipasi, dan menciptakan berbagai dengan disokong oleh teknologi multimedia yang canggih.

Penggunaan sosial media memiliki dampak positif dan negatif. Dampak positif penggunaan sosial media adalah semakin mudahnya informasi dapat diakses dan dibagikan, semakin luasnya jejaring yang dapat diciptakan, semakin mudahnya pembentukan komunitas-komunitas yang berdampak positif bagi masyarakat, maraknya aktifitas *crowdfunding* dan *crowdsourcing*, dan banyak dampak positif lainnya. Di samping dampak positif yang ditimbulkan, penggunaan internet oleh pihak-pihak yang tidak bertanggung jawab (khususnya sosial media) juga dapat menimbulkan dampak negatif. Berbagai kejahatan dapat terjadi di dunia maya yang saat ini dikenal istilah *cybercrime*.

Cybercrime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* adalah kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.¹

Salah satu contoh *cybercrime* adalah tindakan *cyberstalking*. *Cyberstalking* dapat diterjemahkan sebagai penguntitan melalui dunia maya.

*“Cyberstalking involves using the internet, cell phone, and/or any other electronic communication device to stalk another person. Cyberstalking may involve false accusations, threats, identity theft, and damage to data or equipment, solicitation of minors for sexual purposes, and any other form of repeated offensive behavior. It may include ‘creeping,’ in which a person acquires the personal information about another through the internet, typically social networking sites.”*²

¹ Perkasa, R.E., Nyoman, S.P., & Turisno, B. E., “Perlindungan Hukum Pidana Terhadap Konsumen dalam Transaksi Jual Beli *Online* (*E-commerce*) di Indonesia”, *Diponegoro Law Journal*, Vol. 5, No. 4, 2016, hlm 3.

² <https://www.smsu.edu/resources/webspaces/campuslife/counselingtestingservices/cyberstalking.pdf>, diakses tanggal 1 September 2019.

Terjemahan bebas: *Cyberstalking* termasuk tindakan menggunakan internet, telepon selular, dan/atau sarana komunikasi lain untuk menguntit orang lain. *Cyberstalking* dapat termasuk tindakan memberikan tuduhan palsu, ancaman, pencurian identitas, perusakan terhadap data atau peralatan, permintaan anak di bawah umur untuk tujuan seksual, dan segala bentuk perilaku ofensif yang berulang. Perbuatan *cyberstalking* termasuk juga tindakan pergerakan tersembunyi di mana seseorang memperoleh informasi pribadi tentang orang lain melalui internet, biasanya situs jejaring sosial.

Indonesia 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.

Di dalam Pasal 29 dinyatakan bahwa setiap orang dilarang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang **berisi ancaman kekerasan atau menakut-nakuti** yang ditujukan secara pribadi. Pelanggaran terhadap Pasal 27 dan Pasal 29 UU ITE memang dapat dikenai ancaman pidana sebagaimana diatur dalam Pasal 45 UU ITE. Di dalam pasal-pasal UU ITE di atas, disebutkan beberapa unsur delik yang harus dipenuhi untuk menyatakan bahwa tindakan demikian dapat dikenai akibat hukum yaitu adanya unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti.

Pembentuk undang-undang belum mengakomodasi tindakan penguntitan dalam dunia maya (*cyberstalking*), sejauh tindakan pendistribusian informasi elektronik oleh pelaku, tidak mengandung unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti.

Dalam menggunakan sosial media, sangat mungkin terjadi seseorang membuat lebih dari satu akun anonim, dengan identitas yang sengaja ia samarkan, dan akun sosial media tersebut sengaja dibuat untuk mengikuti seseorang. Pelaku menguntit korban misalnya dengan memantau

keseharian dan rutinitas korban, memperhatikan tempat-tempat yang korban datangi secara rutin, mengirimkan pesan, meminta (*request*) pertemanan, dan berusaha untuk dapat berinteraksi dengan korban di dunia nyata. Tindakan seperti itu tidak akan menimbulkan masalah sejauh terdapat persetujuan / *consent* dari orang yang diikuti. Berbeda halnya jika orang yang diikuti merasa terganggu atau bahkan merasa tidak aman dengan penguntitan yang ia alami. Pelaku sama sekali tidak mendistribusikan konten yang melecehkan kesusilaan, menghina atau mencemarkan nama baik, memeras dan/ atau mengancam, ataupun menakut-nakuti. Oleh sebab itu, pelaku tidak dapat dikenai tindakan hukum karena masih terdapat ketidakjelasan, apakah tindakan demikian dapat dikategorikan sebagai pelanggaran hukum.

Penulis tertarik untuk melakukan penelitian ini karena berbagai kasus *cyberstalking* terjadi di dalam masyarakat dan menimbulkan gangguan di tengah-tengah masyarakat. Pelaku melaksanakan tindakannya dengan berbagai modus yang sedemikian rupa sehingga dirinya tidak terkena jerat hukum, khususnya hukum pidana, namun tidak dapat dipungkiri bahwa tindakan yang dilakukan oleh pelaku menimbulkan kerugian bagi korban.

Permasalahan lain yang harus dibahas adalah berkenaan dengan penggunaan akun anonim yang menyulitkan proses penegakan hukum. Dengan demikian, diperlukan analisis lebih lanjut mengenai hal ini. Dengan demikian, permasalahan yang akan dibahas bagaimana sistem hukum pidana Indonesia mengatur tindakan *cyberstalking* yang dilakukan dengan tujuan menimbulkan gangguan dan bagaimana penegakan hukum dapat dilakukan terhadap pelaku *cyberstalking* yang menggunakan akun anonim pada media sosial?

Tulisan ini merupakan hasil penelitian yuridis normatif. yaitu penelitian yang dilakukan dengan langkah melakukan inventarisasi perundang-undangan yang berlaku, mencari asas-asas atau dasar falsafah dari perundang-undangan tersebut, atau penelitian yang berupa usaha penemuan hukum yang sesuai dengan suatu kasus tertentu.³ Dalam penelitian atau pengkajian ilmu hukum normatif, kegiatan untuk menjelaskan hukum tidak diperlukan dukungan data atau fakta-fakta sosial. Penelitian ini menggunakan bahan-bahan hukum yaitu bahan hukum primer berupa peraturan perundang-undangan, dan bahan-bahan hukum sekunder berupa literatur-literatur hukum.

³ Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum*, Bandung: Mandar Maju, 2008, hlm 86.

Sejauh penelusuran yang dilakukan oleh Penulis, berbagai penelitian terkait dengan *cybercrime* dan *cyberstalking* telah banyak dilakukan oleh para peneliti sebelumnya, namun penulis belum menemukan penelitian yang secara khusus membahas bagaimana pertanggungjawaban pidana pemilik akun sosial media anonim yang melakukan tindakan *cyberstalking*, dan pengaturan sanksi pidananya di dalam sistem hukum Indonesia, sehingga diharapkan hasil penelitian ini dapat memberikan kontribusi bagi pengembangan ilmu hukum dan memberikan masukan bagi penyempurnaan regulasi hukum pidana di Indonesia.

PEMBAHASAN

Cyberstalking sebagai suatu *Cybercrime*

Cybercrime merupakan sebuah istilah yang secara sederhana dapat diartikan sebagai kejahatan di dunia maya. Menurut David S. Wall, "*cybercrime broadly describes the crimes that take place within that space and the term has come to symbolize insecurity and risk online.*"⁴ Dalam pengertian di atas, dapat dikatakan bahwa *cybercrime* menunjukkan adanya ketidakamanan dan risiko dalam penggunaan media online. Sebagai sebuah kejahatan, *cybercrime* memenuhi unsur tindakan kejahatan yaitu mengakibatkan terganggunya ketertiban sosial.

*Cybercrime, like crime, consist of engaging in conduct that has been outlawed by a society because it threatens social order. As we will see, most of cybercrime we see today simply represents the migration of real-world crime into cyberspace.*⁵ Kejahatan yang semula dilakukan di dunia nyata, dipindahkan tempat terjadinya ke dalam *cyberspace*. Semula, berbagai kejahatan tersebut dilakukan secara fisik, di mana terjadi pertemuan langsung antara pelaku dan korban. Misalnya, tindakan pencurian, penipuan, pengancaman, penghinaan, pelecehan seksual, dan sebagainya.

Kejahatan yang menggunakan teknologi berbasis komputer dan jaringan telekomunikasi dapat dikelompokkan ke dalam beberapa jenis, yaitu:

1. *Unauthorized Access to Computer System and Service*: akses ilegal terhadap sistem dan layanan komputer;
2. *Illegal Contents*: konten ilegal;

⁴ David S. Wall, *Cybercrime, The Transformation of Crime in the Information Age*, United Kingdom: Polity Press, 2007, hlm 10.

⁵ Susan W. Brenner, *Cybercrime and The Law, Challenges, Issues and Outcomes*, Boston: Northeastern University Press, 2012, hlm 6.

3. *Data Forgery*: pencurian data;
4. *Cyber Espionage*: spionase;
5. *Cyber Sabotage and Extortion*: sabotase dan pemerasan;
6. *Offense against Intellectual Property*: pelanggaran hak kekayaan intelektual;
7. *Infringements of Privacy*: pelanggaran privasi.

Sebelum memulai pembahasan lebih mendalam mengenai tindakan penguntitan di dunia maya sebagaimana dijelaskan dalam latar belakang tulisan ini, perlu dibahas terlebih dulu, pengertian / definisi dari konsep *cyberstalking*. Hal ini bertujuan untuk memberikan batasan mengenai tindakan seperti apa yang termasuk dalam kategori *cyberstalking*. Terdapat berbagai definisi dari para ahli terkait dengan *cyberstalking*, sebagai berikut:

Menurut Black's Law Dictionary 11th edition, *cyberstalking* adalah:

*“the act of threatening, harassing, or annoying someone through multiple e-mail messages, as through the internet, esp with the intent 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.”*⁶

Terjemahan:

“tindakan mengancam, melecehkan, **atau** mengganggu seseorang melalui berbagai pesan e-mail, seperti melalui internet, khususnya dengan maksud menempatkan penerima dalam ketakutan akan terjadinya tindakan ilegal atau tindakan yang dapat menimbulkan cedera pada penerima atau anggota keluarganya”

Dari rumusan di atas, maka unsur-unsur utama dari *cyberstalking* adalah:

1. *act of threatening, harassing, or annoying someone*: tindakan mengancam, melecehkan, atau mengganggu seseorang
2. *through internet*: melalui internet
3. *with the intent of placing the recipient with fear of an illegal act or injury*: dengan maksud membuat korban takut akan tindakan ilegal atau luka.⁷

⁶ Bryan A. Garner, *Black's Law Dictionary 11th edition*, United States: Thomson West; Aspatore Books, 2019.

⁷Shanti Rachmadsyah, *Cyberstalking*, dalam situs:

<https://www.hukumonline.com/klinik/detail/ulasan/lt4bd5f301cea84/cyberstalking/> , diakses tanggal 18 September 2019, pkl. 11.44.

Dari definisi di atas, terdapat unsur *threatening* (mengancam). Namun unsur ancaman tersebut hanya merupakan salah satu unsur dari *cyberstalking*, di samping unsur *harrasing* (melecehkan) atau *annoying* (menggangu). Keberadaan kata “atau” bermakna alternatif. Berarti, *cyberstalking* sudah terjadi jika tindakan sudah memenuhi salah satu dari ketiga unsur mengancam, melecehkan atau menggangu.

Di bawah ini akan dijelaskan secara singkat pengertian dari unsur *threatening* (mengancam), *harrasing* (melecehkan) atau *annoying* (menggangu), khususnya dalam konteks penggunaan media online sebagai sarana.

1. *Threatening* (mengancam)

Di dalam sistem hukum Indonesia, terminologi “pengancaman” dapat ditemukan misalnya di dalam Kitab Undang-undang Hukum Pidana. Dalam Pasal 368 (1) KUHP ditemukan istilah “ancaman kekerasan”, dan di dalam Pasal 369 (1) KUHP ditemukan istilah “ancaman pencemaran”.

Pasal 368(1) KUHP menyatakan: Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, **memaksa** seseorang dengan kekerasan atau **ancaman kekerasan**, untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya memberi hutang maupun menghapuskan piutang diancam karena pemerasan, dengan pidana penjara paling lama sembilan tahun.

Pasal 369 (1) KUHP menyatakan: Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan **ancaman pencemaran** baik dengan lisan maupun tulisan atau dengan ancaman akan membuka rahasia, memaksa seorang untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya memberi hutang maupun menghapuskan piutang diancam, dengan pidana penjara paling lama empat tahun.

Kedua pasal di atas mengandung unsur subjektif berupa maksud seseorang untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Adapun unsur objektifnya adalah berupa tindakan memaksa dengan kekerasan, mengancam akan melakukan kekerasan (Pasal 368 ayat (1)); tindakan mengancam untuk melakukan pencemaran (Pasal 369 ayat (1)). Intinya, unsur ancaman adalah unsur di mana seseorang menakut-nakuti orang lain, menempatkan orang lain di bawah tekanan sehingga orang

tersebut (korban), mengikuti apa yang diminta oleh pelaku. Di dalam UU ITE, istilah “ancaman” ditemukan dalam Pasal 29 dan Pasal 45 B.

Pasal 45 B: 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 dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Penjelasan Pasal 45 B: Ketentuan dalam Pasal ini termasuk juga di dalamnya perundungan di dunia siber (*cyber bullying*) yang mengandung unsur ancaman kekerasan atau menakut-nakuti dan mengakibatkan kekerasan fisik, psikis, dan/atau kerugian materiil. Pengancaman merupakan sebuah tindakan mengancam. Mengancam, menurut Kamus Besar Bahasa Indonesia adalah tindakan menyatakan maksud (niat, rencana) untuk melakukan sesuatu yang merugikan, menyulitkan, menyusahkan, atau mencelakakan pihak lain.⁸ Ancaman akan berdampak munculnya tekanan pada diri korban, baik tekanan tersebut berupa tekanan fisik atau psikis.

Terkait dengan keberadaan unsur ancaman, di mana ancaman tersebut secara subjektif akan dirasakan oleh korban, dan berdasarkan hal tersebut korban akan memutuskan apakah dirinya merasa perlu untuk melanjutkan kasus ini melalui jalur hukum pidana, maka kemudian perlu dibedakan terlebih dahulu adanya klasifikasi delik yaitu sebagai delik biasa dan delik aduan (*klachtdelict*). Pada prinsipnya, *klachtdelict* adalah tindakan-tindakan pidana yang penuntutannya dapat dilakukan berdasarkan pengaduan dari pihak yang dirugikan. *Klachtdelict* dibedakan menjadi:

“a. *Klachtdelict* yang bersifat relatif, artinya dalam nentuk umum ia bukan *klachtdelict*, tetapi karena sesuatu hal dianggap *klachtdelict*, misalnya Pasal 367 tentang pencurian dalam keluarga. Pencurian bukanlah *klachtdelict*, tetapi bila pencurian itu dilakukan dalam keluarga, dia menjadi *klachtdelict*.

b. *Klachtdelict* yang bersifat mutlak, artinya memang selamanya memerlukan penaduan misalnya Pasal 284 (perzinahan)”⁹

⁸ <https://kbbi.kemdikbud.go.id>, diakses tanggal 11 September 2019, pk. 08.00.

⁹ H.M, Rasyid Ariman dan Fahmi Raghil, *Hukum Pidana*, Malang: Setara Press, 2015, hlm. 83.

2. *Harrasing* (melecehkan)

Menurut Kamus Besar Bahasa Indonesia, melecehkan berarti: memandang rendah (tidak berharga); menghinakan; mengabaikan¹⁰. 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 penelusuran terhadap *Report of Online Harassment, Digital Abuse, And Cyberstalking In America* yang diterbitkan oleh *Center for Innovative Public Health Research* pada tahun 2016, ditemukan pengertian sebagai berikut:

“Defining online harassment and abuse Harassment can encompass a wide range of unwanted contact that is used to create an intimidating, annoying, frightening, or even hostile environment for the victim. Online harassment is generally recognized as referring to this type of negative and unwanted contact using digital means. Online harassment can be a brief occurrence or a sustained campaign of abuse and attacks; the perpetrator (or perpetrators) might be intimately known to the victim, or a stranger in another state or country. Online harassment is defined less by the specific behavior than its intended effect on and the way it is experienced by its target. While some forms of online harassment are quite similar to their “offline” equivalents, the internet can make other forms of harassment easier to accomplish. In terms of cyberstalking, for instance, stalkers can monitor and contact their victims through a number of digital channels. Digital tools also allow for new types of harassment that were either not previously possible or take on a fundamentally different character in an online context. As Danah Boyd has outlined, certain characteristics of networked online spaces change the dynamics of interaction on these platforms. For example, the ability to post comments anonymously versus having to take ownership of one’s ideas can affect the culture and context of the online space. Moreover, the persistence and searchability of online environments means that many forms of online harassment can remain online indefinitely, accessible and connected with the victim. Meanwhile, the replicability and scalability of networked spaces can make it easier for strangers to join in on the abuse.”
11

Dari uraian di atas, penulis menekankan beberapa unsur pokok dalam tindakan pelecehan secara online yaitu:

- a) *unwanted contact*: adanya kontak yang tidak diinginkan

¹⁰ *Ibid.*

¹¹ Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, Myeshia Price-Feeney, “Online Harassment, Digital Abuse, And Cyberstalking in America”, *Center for Innovative Public Health Research*, hlm 8.

- b) tujuan dari dilakukannya kontak: untuk menciptakan lingkungan yang mengintimidasi, menyebarkan, menakutkan bagi korban.
- c) Dalam hal *cyberstalking*, penguntit dapat memantau dan menghubungi korban mereka melalui sejumlah saluran digital, dengan modus mengirim komentar secara anonim.
- d) Tindakan pelecehan terjadi secara online dan tanpa batas.

3. *Annoying* (menggangu)

Kata *annoying* (menggangu) merupakan kata yang bermakna negatif. Menurut Oxford Dictionary, *annoying* berarti *making somebody feel slightly angry*, atau membuat seseorang merasa **sedikit** marah. Dalam Kamus Besar Bahasa Indonesia, kata menggangu diartikan:

- 1) menggoda; mengusik:
- 2) merintang; menyebabkan tidak berjalan sebagaimana mestinya (tentang keadaan umum, kesehatan badan, dan sebagainya
- 3) merisaukan (tentang hati, pikiran
- 4) merusak suasana:
- 5) mendatangkan kekacauan (kerusakan dan sebagainya).

Dari definisi yang diuraikan, muncul kesan bahwa level kerugian yang ditimbulkan oleh tindakan “menggangu”, nampaknya tidak sedemikian serius dibandingkan dengan kerugian yang timbul dari tindakan mengancam dan melecehkan. Pembentuk undang-undang pun mengatur bahwa pengguna internet akan mendapatkan sanksi jika melakukan tindakan yang memenuhi unsur mengancam dan / atau melecehkan. Hal inilah yang membuat banyak orang merasa bahwa tindakan menggangu orang lain melalui media internet adalah tindakan yang tidak menyalahi hukum. Padahal, setiap pengguna internet sebagai anggota masyarakat harus mendapatkan jaminan keamanan dan kenyamanan dalam melaksanakan aktivitasnya di dunia maya tersebut. Dalam sub bab selanjutnya, penulis akan mencoba menguraikan apakah tindakan penguntitan di dunia maya yang hanya bersifat menggangu, layak dikategorikan sebagai tindakan melawan hukum.

Unsur-unsur Tindakan *Cyberstalking*

Hukum pidana berlandaskan asas legalitas sebagaimana tercantum di dalam Pasal 1 ayat (1) Kitab Undang-undang Hukum Pidana (KUHP) yang menyatakan bahwa tiada suatu perbuatan

dapat dipidana kecuali atas kekuatan berlakunya aturan tertulis yang ada sebelum perbuatan dilakukan. Menurut Profesor Pompe, bahwa menurut hukum positif kita, suatu *strafbaar feit* itu sebenarnya adalah tidak lain daripada suatu tindakan yang menurut sesuatu rumusan undang-undang telah dinyatakan sebagai tindakan yang dapat dihukum.¹² Dengan demikian, setiap tindakan dapat disebut sebagai tindak pidana hanya jika melanggar aturan tertulis. Untuk menentukan apakah suatu tindakan melanggar aturan pidana atau tidak, perlu dilihat apakah tindakan tersebut memenuhi unsur yang disyaratkan.

Sampai saat ini, tindakan *cyberstalking* tanpa adanya unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti, belum dapat dikenai hukuman. Unsur “menggangu” belum menjadi dasar yang cukup untuk mengenakan sanksi pidana bagi pelaku.

Jika diteliti lebih lanjut, pelaku *cyberstalking* biasanya melakukan tindakan seperti berikut:

- 1) Membuat akun sosial media anonim, menggunakan nama samaran, dan mengoperasikan akun tersebut dengan sengaja untuk menguntit orang lain.
- 2) Mengirimkan pesan kepada korban, di mana isi pesan berupa ajakan untuk berinteraksi atau bahkan bertemu, pernyataan perasaan, dan sebagainya.
- 3) Pelaku mengikuti semua informasi yang ditulis oleh korban / sasarannya, melalui akun sosial media milik korban.
- 4) 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.)
- 5) 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.

Perihal modus operandi yang dilakukan oleh *cyberstalker*, Siemieniecka & Skibinska menguraikan pernyataan di bawah ini:

¹² PAF. Lamintang, *Dasar-dasar Hukum Pidana Indonesia*, Bandung: Citra Aditya Bakti, 1996, hlm 183.

*“Forms of victim harrasment take the form of: frequent phone calls, sending innumerable message, sending unwanted presents, parcels, intrusive meetings, tripsi, sexual proposal, victim tracking, overrides at workplace, or place of residence, emotional blackmail, etc.”*¹³

Pelaku *cyberstalking* dapat diklasifikasikan menjadi beberapa tipe sebagai berikut: ¹⁴

- 1) *Vindictive cyberstalker*, pelaku melakukan pengancaman dan pelecehan kepada korban, melakukan *spamming*, pengiriman *e-mail* berturut-turut, pencurian identitas.
- 2) *Composed cyberstalker*, pelaku melakukan tindakannya dengan perilaku-perilaku yang tenang. Tujuan utamanya memberikan tekanan yang terus menerus (secara konstan) dengan perilaku perilaku yang cenderung mengancam.
- 3) *Intimate cyberstalker*, pelaku ingin memiliki hubungan dengan targetnya berdasarkan obsesi yang muncul pada dirinya.
- 4) *Collective cyberstalker*, di mana dua atau lebih pelaku memiliki target yang sama.

Salah satu contoh kasus nyata, terjadi di Bandung pada bulan September 2019, di mana seorang pria menguntit seorang wanita dan wanita tersebut menyatakan penolakan dengan mem-*block* akun sosial media dari pria tersebut. Merasa sakit hati, pelaku penguntitan melakukan penusukan pada korban. Pelaku dapat dijerat pasal pidana penganiayaan, namun belum ada aturan yang jelas yang dapat dikenakan terhadap tindakan penguntitan yang dilakukannya.¹⁵

Jika dilihat dari hal-hal yang diperbuat oleh pelaku penguntitan, dikaitkan dengan pandangan hukum pidana, penulis berpendapat bahwa:

- 1) Telah terjadi tindakan yang disengaja. Perbuatan didasari oleh unsur *opzet/dolus*. Pengertian “sengaja” adalah suatu sikap batin di mana pelaku mengetahui dan menghendaki tindakan yang dilakukannya. Tindakan ini bukan didasari oleh sikap kelalaian atau kurang hati-hatian. Unsur kesengajaan ini juga disyaratkan di dalam Pasal 45 B UU ITE di mana informasi elektronik dengan muatan ilegal yang dikirimkan, didasari oleh sikap batin “sengaja”.

¹³ Siemieniecka & Skibinska, “Stalking and Cyberstalking a Form of Violence”, *Proceeding of The International Scientific Conference*, Volume III, 2019, hlm. 408.

¹⁴ Michael Pitaro, “Cyberstalking: An Analysis of Online Harrasment and Intimidation”, *International Journal of Cyber Criminology*, Vol 1. Issue 2, 2007, hlm. 188.

¹⁵ <https://nasional.republika.co.id/berita/pxm5nq384/siswi-smk-di-kota-bandung-ditusuk-saat-akan-masuk-sekolah>, diakses tanggal 18 September 2019, pk. 13.00 WIB.

- 2) Telah terjadi tindakan yang merugikan orang lain. Korban mungkin merasa terancam karena terus menerus diikuti, walaupun pelaku tidak mengeluarkan kalimat yang mengancam atau melakukan tindakan fisik yang mengancam. Setiap tindakan yang dirumuskan dalam KUHP maupun UU ITE sebagai tindak pidana, merupakan tindakan yang merugikan orang lain.
- 3) Korban telah secara eksplisit menyatakan penolakan terhadap perbuatan pelaku, dan/atau telah melakukan tindakan untuk menutup akses interaksi dengan pelaku (misal, melakukan pengaturan privasi pada akun miliknya. Hal ini menunjukkan bahwa di dalam tindakan yang dilakukan oleh pelaku terdapat unsur paksaan, karena tidak terdapat *consent* / persetujuan dari korban. Pasal 368 (1) KUHP juga mengkualifikasikan tindakan pemaksaan sebagai tindak pidana.
- 4) Gangguan yang diberikan ditujukan pada pribadi. Sulit untuk mengategorikan apakah tindakan semacam ini layak dikategorikan sebagai “kejahatan”, karena makna kata “mengganggu” bersifat sangat relatif. Tingkat keseriusan terkait akibat yang timbul dari gangguan juga bersifat subjektif, tergantung pada apa yang dirasakan oleh korban. Demikian tindakan ini akan lebih tepat dikualifikasikan sebagai delik aduan.

Dengan demikian, dipandang dari perspektif perbuatan, penulis berpendapat bahwa terpenuhinya unsur perbuatan yang disengaja, dan menimbulkan kerugian bagi orang lain, menjadikan perbuatan ini layak ditetapkan sebagai suatu perbuatan yang melawan hukum. Perlu pengaturan lebih lanjut mengenai prosedur penindakan, mengingat perbuatan ini dilakukan di balik sebuah akun sosial media anonim. Di samping itu, perlu dipertimbangkan pula aspek kejiwaan pelaku untuk memastikan kemampuannya bertanggung jawab secara hukum.

Mengutip pendapat dari M. Ainul Syamsu, bahwa konsiderasi tindak pidana dan pertanggungjawaban pidana sebagai dasar penjatuhan pidana memberikan kekuasaan yang seimbang antara legislator dan pengadilan. Ancaman pidana merefleksikan kebijakan legislator dalam merumuskan tindak pidana bersandar kepada standar umum masyarakat. Dalam konteks ini, penjatuhan pidana yang hanya mendasarkan kepada tindak pidana semata berarti meletakkan pengadilan sebagai corong undang-undang. Hal ini sangat berbeda manakala penjatuhan pidana dipandang sebagai kebijakan pengadilan yang bertujuan untuk menyeimbangkan standar umum

masyarakat yang terkandung dalam tindak pidana dan keadaan pribadi pembuat tindak pidana yang terkandung dalam kesalahan dan pertanggungjawaban pidana.¹⁶

Pernyataan tersebut bermakna bahwa dalam hal ini, walaupun tindakan pelaku telah memenuhi unsur perbuatan melawan hukum, di dalam penegakan sanksinya tetap diperlukan kebijaksanaan dari hakim untuk mempertimbangkan apakah pelaku berada di dalam kondisi pribadi yang memungkinkan dirinya untuk bertanggungjawab secara pidana. Diperlukan informasi tentang kondisi kejiwaan pelaku, apakah pelaku yang melakukan tindakan penguntitan secara terus menerus memiliki gangguan psikis atau tidak. Untuk memahami hal ini tentunya memerlukan pendekatan multidisiplin, yakni dengan melibatkan psikolog dan/psikiater untuk memeriksa kondisi kejiwaan pelaku.

Penegakan Hukum Pidana Bagi Pelaku *Cyberstalker* yang menggunakan Akun Anonim

1. Tentang *Anonymous Account* dan Pertanggungjawaban Hukum Pidana

Hukum pidana merupakan bagian dari hukum publik yang mengatur tindakan seseorang, menetapkan perbuatan yang dilarang, dan menetapkan sanksi atas pelanggaran dari perbuatan itu. Berdasarkan asas legalitas, hukum pidana melalui peraturan tertulis menetapkan tindakan apa saja yang dilarang, kemudian menetapkan sanksi atas pelanggaran-pelanggaran yang dilakukan oleh pelaku tindak pidana tersebut.

Pelaku dapat dikenai sanksi dengan dasar pemikiran bahwa yang bersangkutan adalah subjek hukum yang mampu bertanggung jawab. Pertanggungjawaban lahir dari tindakan seseorang yang mampu bertanggungjawab, yaitu orang yang menyadari perbuatannya dan akibat dari perbuatannya.

Mengenakan pertanggungjawaban pidana terhadap manusia dalam interaksi di dunia nyata bukan merupakan hal yang problematis. Penegak hukum, melalui mekanisme hukum acara yang berlaku, dapat melakukan penyelidikan dalam rangka menemukan terjadinya tindak pidana, dan tahap penyidikan dalam rangka mencari dan menemukan tersangka. Terhadap tersangka, kemudian dapat dilakukan tindakan penangkapan, penahanan dan proses-proses hukum lainnya sampai dengan dijatuhkannya vonis.

¹⁶ M.Ainul Syamsu, *Penjatuhan Pidana dan Dua Prinsip Hukum Pidana*, Jakarta: Kencana Prenada Media, 2016, hlm. 11.

Lain halnya dengan pelaku tindak pidana di dunia nyata, pelaku tindak pidana di dunia maya melakukan tindakannya dengan perantaraan sebuah akun atau lebih. Idealnya, sebuah akun haruslah menjadi wadah atau sarana tersedianya informasi elektronik yang akurat tentang identitas diri dari pengguna / pemilik akun tersebut. Sebagai contoh, seseorang membuat akun e-mail, yang dapat dimanfaatkan untuk mengirim dan menerima pesan. Kemudian, ketika ia akan membuat akun sosial media, dirinya diminta untuk mendaftarkan alamat e-mailnya, dan melakukan beberapa langkah verifikasi data sampai akhirnya akun sosial media tersebut dapat ia gunakan.

Dalam kenyataannya, saat ini dengan mudah seseorang dapat membuat akun sosial media secara anonim, menggunakan nama samaran sehingga segala aktivitas yang dilakukan atas nama sosial media itu menjadi sulit dipertanggungjawabkan karena tidak jelas, siapa sebenarnya yang ada di balik akun tersebut. Sampai saat ini, pembuatan akun media sosial secara anonim di Indonesia masih sulit dicegah. Salah satu penyebabnya adalah karena platform sosial media hanya menyimpan data alamat e-mail pengguna, sehingga dalam hal terjadi penyalahgunaan sosial media oleh akun anonim, penegakan hukum menjadi sulit dilaksanakan.

Berbagai perbuatan melawan hukum dapat terjadi di balik sebuah akun media sosial anonim. Di Indonesia, banyak sekali dijumpai akun-akun sosial media yang dibuat secara tidak bertanggungjawab dan dimanfaatkan untuk menyerang pribadi orang lain, baik untuk menyerang publik figur ataupun masyarakat biasa. Akun-akun tersebut dapat juga dimanfaatkan untuk menyerang nama baik orang lain, menjadi sarana ujaran kebencian / *hate speech*. Kasus-kasus terkait akun anonim yang marak dijumpai misalnya bermunculan akun-akun media sosial yang oleh masyarakat dikenal sebagai “akun gosip” dan “akun *haters*”. Pemilik akun / pengelola akun dengan sengaja mencari berita dengan menguntit orang lain, bahkan secara sembunyi-sembunyi mengikuti orang lain, mengambil gambar atau video dan menyebarkanluaskannya kepada khalayak. Akun-akun tersebut dapat dikategorikan sebagai akun anonim karena identitas pemilik dan penanggungjawab akun tersebut tidak jelas.

Pengaturan mengenai akun anonim di dalam UU ITE, terdapat di dalam Pasal 35 yang menyatakan:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen

Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

Dengan sanksi sebagaimana diatur dalam Pasal 51 UU ITE:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Dengan demikian, pengaturan tentang larangan pembuatan akun anonim sudah ada di dalam sistem hukum Indonesia, hanya saja penerapan pertanggungjawaban hukum bagi pembuat akun anonim masih sulit dilakukan. Hal ini disebabkan belum terdapat sistem pendataan pengguna internet yang kredibel, di mana setiap orang dapat membuat akun media sosial dengan berbekal identitas palsu, dan sistem elektronik dari aplikasi media sosial saat ini belum menerapkan sistem verifikasi data yang andal, untuk memastikan keaslian identitas pengguna.

Hukum pidana mensyaratkan terpenuhinya unsur “setiap orang” atau “barangsiapa” di dalam rumusan delik. Penggunaan akun anonim akan menyulitkan terbuktinya unsur “setiap orang”, karena siapa orang yang dimaksud sulit terdeteksi dan sulit untuk dilakukan proses hukum selanjutnya.

2. Problematika Kriminalisasi Tindakan *Cyberstalking* Yang Dilakukan Oleh Pemilik Akun Anonim

Hukum pidana merupakan hukum publik yang melibatkan campur tangan negara di dalam penegakannya. Demikian pula negara berperan dalam menetapkan kebijakan hukum pidana sesuai dengan tujuan yang ingin dicapai, yakni untuk menanggulangi kejahatan. Oleh sebab itu negara juga berperan dalam menetapkan perbuatan apa saja yang dikualifikasikan sebagai tindak pidana. Negara memiliki peranan dalam menerapkan kebijakan kriminalisasi.

Sebagai usaha penanggulangan kejahatan, politik kriminal dapat diwujudkan dalam pelbagai bentuk. Bentuk yang pertama adalah bersifat represif yang menggunakan sarana penal, yang sering disebut sebagai sistem peradilan pidana (*criminal justice system*). Dalam hal ini secara luas sebenarnya mencakup pula proses kriminalisasi. Yang kedua berupa usaha-usaha *prevention without punishment* (tanpa menggunakan sarana penal), dan yang ketiga adalah

mendayagunakan usaha-usaha pembentukan opini masyarakat tentang kejahatan dan sosialisasi hukum melalui mass media secara luas¹⁷.

Pada prinsipnya, hukum pidana bersifat *ultimum remedium*. Hukum pidana selayaknya menjadi upaya terakhir untuk menyelesaikan suatu perkara. Tidak semua tindakan yang dianggap dapat menimbulkan kerugian, harus dinyatakan sebagai tindak pidana. Dengan demikian, proses kriminalisasi harus dilakukan dengan sangat cermat.

Dengan demikian, sebelum menetapkan ancaman pidana, haruslah diperhatikan hal-hal di bawah ini:

1. Bahwa tujuan hukum pidana adalah untuk menanggulangi kejahatan.
2. Bahwa perbuatan yang tidak merugikan, tidaklah dapat ditetapkan sebagai perbuatan pidana, dan tidak semua perbuatan yang merugikan perlu dipidana.
3. Bahwa aturan yang ditetapkan tidak boleh memberikan beban sosial (*social cost*) yang tinggi, sehingga tidak sebanding dengan hasil yang akan diperoleh.
4. Bahwa negara dapat memastikan kemampuan badan penegak hukum yang akan menegakan aturan tersebut.

Penulis berpendapat bahwa apabila tindakan *cyberstalking* yang dilakukan oleh pemilik akun anonim tanpa adanya unsur *illegal content* (pelanggaran kesusilaan, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti) dikriminalisasi, maka perlu diperhatikan:

1. Bahwa jika tindakan demikian akan dikriminalisasikan, maka jenis delik yang sesuai adalah delik aduan. Delik aduan merupakan delik yang penuntutannya dapat dilakukan berdasarkan aduan dari pihak yang dirugikan. Hal ini mengingat bahwa gangguan yang ditimbulkan oleh tindakan ini lebih mengarah ke gangguan terhadap pribadi seseorang dan tidak langsung berpengaruh pada kepentingan publik. Dengan demikian, perlu dibatasi sejauh mana negara dapat melakukan intervensi terhadap penindakan delik ini.
2. Proses penegakan hukum akan berjalan jika ditunjang dengan sistem yang baik, termasuk keberadaan struktur dan lembaga penegak hukum yang memadai. Negara perlu menyusun bagaimana mekanisme pelacakan pelaku yang menggunakan akun anonim, sehingga pelaku dapat tertangkap dan hukum pidana dapat ditegakan kepadanya.

¹⁷ Sudarto. *Hukum dan Hukum Pidana*. Bandung: Alumni, 2007, h. 36.

3. 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 *screenshot* pesan yang dikirim, bukti riwayat interaksi melalui media sosial, sehingga diperlukan pengaturan mengenai pembuktian untuk tindak pidana ini.

Kriminalisasi tidak dapat dilakukan secara sembarangan. Asas yang harus tetap menjadi pedoman adalah asas legalitas (*nullum delictum, nulla poena sine praevia lege poenali*) yang dikemukakan oleh von Feurbach. Ungkapan itu mengandung pengertian bahwa “tidak ada suatu perbuatan yang dapat dipidana kecuali atas perundang-undangan pidana yang sudah ada sebelum perbuatan itu dilakukan”. Asas legalitas adalah asas yang paling penting dalam hukum pidana, khususnya asas pokok dalam penetapan kriminalisasi.

PENUTUP

Berdasarkan uraian yang telah dipaparkan pada bagian sebelumnya, penulis menarik simpulan bahwa diperlukan pengaturan yang lebih jelas tentang tindakan *cyberstalking*. Dengan demikian, untuk mengatasi problematika pengaturan *cyberstalking* ini, diperlukan aturan hukum pidana yang dengan tegas merumuskan barangsiapa dengan sengaja melakukan penguntitan kepada orang lain melalui media internet, mengirimkan informasi elektronik secara pribadi kepada orang lain, dan tindakannya menimbulkan gangguan terhadap diri orang lain tersebut, diancam dengan ancaman pidana. Namun, tindakan *cyberstalking* perlu dikriminalisasi dengan batas-batas yang jelas, yaitu dengan mengkuifikasikannya sebagai delik aduan, dan dalam penjatuhan sanksi, penegak hukum harus memperhatikan kondisi kejiwaan dari pelaku.

Penegakan hukum untuk kasus *cyberstalking* yang dilakukan oleh akun anonim di Indonesia dapat dilaksanakan dengan terlebih dahulu dilakukan pembenahan terkait pengaturan verifikasi identitas pengguna internet oleh penyedia sistem elektronik, sehingga walaupun akun media sosial dibuat dengan nama samaran atau tanpa nama, penegak hukum tetap dapat mengetahui siapa orang yang bertanggungjawab atas segala perbuatan melawan hukum yang terjadi di balik akun media sosial anonim tersebut.

Untuk mengatasi dan mengantisipasi berbagai permasalahan yang timbul sehubungan dengan penggunaan akun anonim secara tidak bertanggungjawab, maka negara perlu mengatur

mekanisme verifikasi identitas di mana setiap penyelenggara sistem elektronik diwajibkan melakukan verifikasi pengguna melalui *e-mail* dan nomor telepon, termasuk jika diperlukan, memasukan data nomor induk kependudukannya, sehingga dapat dipastikan bahwa pengguna akun termasuk pengguna akun media sosial tidak menggunakan identitas fiktif. Namun, pengaturan ini harus ditunjang juga dengan sistem perlindungan data pribadi sehingga tidak menimbulkan permasalahan baru terkait dengan penyalahgunaan data pribadi pengguna internet.

DAFTAR PUSTAKA

Buku

- Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum*, Bandung: Mandar Maju, 2008.
- David S. Wall, *Cybercrime, the Transformation of Crime in the Information Age*, United Kingdom: Polity Press, 2007.
- H. M. Rasyid Ariman dan Fahmi Raghieb, *Hukum Pidana*, Malang: Setara Press, 2015.
- M. Ainul Syamsu, *Penjatuhan Pidana dan Dua Prinsip Hukum Pidana*, Jakarta: Kencana Prenada Media, 2016.
- PAF. Lamintang, *Dasar-dasar Hukum Pidana Indonesia*, Bandung: Citra Aditya Bakti, 1996.
- Sudarto, *Hukum dan Hukum Pidana*, Bandung: Alumni, 2007.
- Susan W. Brenner, *Cybercrime and the Law, Challenges, Issues and Outcomes*, Boston, Northeastern University Press, 2012.

Jurnal

- Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, Myeshia Price-Feeney, "Online Harassment, Digital Abuse, and Cyberstalking in America", *Center for Innovative Public Health Research*, 2016.
- Michael Pitaro, "Cyberstalking: An Analysis of Online Harassment and Intimidation", *International Journal of Cyber Criminology*, Vol 1. Issue 2, 2017.
- Perkasa, R.E., Nyoman, S.P., & Turisno, B.E, "Perlindungan Hukum Pidana Terhadap Konsumen dalam Transaksi Jual Beli *Online (E-commerce)* di Indonesia", *Diponegoro Law Journal*, Vol. 5, No. 4, 2016.
- Siemieniecka & Skibinska, "Stalking and Cyberstalking a Form of Violence", *Proceeding of The International Scientific Conference*, Volume III, 2019.

Perundang-Undangan

Kitab Undang-undang Hukum Perdata.

Kitab Undang-undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Kamus

Bryan A. Garner, *Black's Law Dictionary 7th edition*, United States, Thomson West; Aspatore Books, 2014.

Pranala Luar

<https://www.hukumonline.com/klinik/detail/ulasan/lt4bd5f301cea84/cyberstalking/>

<https://kbbi.kemdikbud.go.id>

<https://www.smsu.edu/resources/webspaces/campuslife/counselingtestingservices/cyberstalking.pdf>

<https://nasional.republika.co.id/berita/pxm5nq384/siswi-smk-di-kota-bandung-ditusuk-saat-akan-masuk-sekolah>