**KRTHA BHAYANGKARA, Vol. 16, No. 1 (2022), pp. 163-176**
ISSN 1978-8991 (print) | ISSN 2721-5784 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/KRTHA

# *Cyberstalking*: Kejahatan Terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana

**Amelia Putri Anisah[1*], Eko Nurisman[2]**

[12]Fakultas Hukum, Universitas Internasional Batam, Indonesia
Email: 1951020.Amelia@uib.edu
*Corresponding author

**Article info**

| Received: Mar 3, 2022 | Revised: Apr 8, 2022 | Accepted: Apr 11, 2022 |
|---|---|---|

DOI: https://doi.org/10.31599/krtha.v16i1.1047

**Keywords :** *personal data protection, technology, cyberstalking*

**Abstract :** *The rapid development is marked by changes in telecommunications technology and computer technology. Technological sophistication gives rise to various kinds of crimes aimed at the virtual world community, one form of crime that occurs is cyberstalking. From this phenomenon, it is necessary to describe several arrangements that serve as the basis for tackling the rapid rate of cyberstalking. This research employs a normative judicial approach based on legal data gleaned from research sources. The primary and secondary legal information used in this research are both primary and secondary. The law number contains the majority of the legal information. 1. Amendments to the Information and Electronic Transactions Law No. 11 of 2008 (UU ITE) No. 19 of 2016 on Information and Electronic Transactions (UU ITE). Obtain secondary legal materials through library research, such as books, legal publications, the Internet, and expert opinion. The results of this study show that due to the rapid development of technology, many crimes stem from technological sophistication, including those related to cyberstalking, so it requires a special regulation that regulates cyberstalking, while there is no special regulation in tackling cyberstalking crimes. Regulations related to cyberstalking are still adopting the provisions of the ITE Law No. 19 of 2016 amendments to the ITE Law No. 11 of 2008.*

**Kata kunci :** perlindungan data pribadi, teknologi, cyberstalking

**Abstrak :** Pesatnya perkembangan ditandai dengan perubahan-perubahan akan teknologi telekomunikasi dan teknologi komputer. Kecanggihan teknologi memunculkan berbagai macam kejahatan yang dituju kepada masyarakat dunia maya, salah satu bentuk kejahatan yang terjadi berupa cyberstalking. Dari fenomena ini perlu dijabarkan beberapa pengaturan yang dijadikan sebagai landasan dalam menanggulangi pesatnya tindakan cyberstalking. Penelitian ini menggunakan pendekatan yuridis normatif berdasarkan data hukum yang diperoleh dari sumber-sumber penelitian. Informasi hukum primer dan sekunder yang digunakan dalam penelitian ini bersifat primer dan sekunder. Nomor hukum berisi sebagian besar informasi hukum. 1. Perubahan Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 (UU ITE) Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Memperoleh bahan hukum sekunder melalui penelitian kepustakaan, seperti buku, publikasi hukum, internet, dan pendapat ahli. Hasil penelitian ini memperlihatkan bahwa atas berkembangnya

teknologi yang begitu pesat banyak memunculkan kejahatan-kejahatan yang bersumber pada kecanggihan teknologi diantaranya terkait tindakan cyberstalking, sehingga memerlukan suatu peraturan khusus yang mengatur tindakan cyberstalking, sementara itu belum terdapatnya pengaturan khusus dalam menanggulangi kejahatan cyberstalking. Pengaturan terkait cyberstalking masih mangadopsi pengaturan pada UU ITE No 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008.

## I. PENDAHULUAN

Pesatnya perkembangan zaman ditandai dengan perubahan teknologi telekomunikasi dan komputer yang diyakini dapat memberikan dampak positif bagi kehidupan masyarakat. Perkembangan itu dapat menghasilkan jaringan internet yang multifungsi. Keserbagunaan ini membuktikan bahwa keberadaan teknologi internet dapat mempermudah pertukaran informasi masyarakat. Jaringan Internet multifungsi, di sisi lain, memiliki dampak positif dan negatif pada kehidupan sosial. Maraknya internet dapat berdampak negatif, karena sebagian pengguna internet melakukan aksi *stalking* seseorang secara *online*, istilah yang dikenal dengan *cyberstalking.*

Berbagai perubahan dalam norma komunikasi dan interaksi sosial telah muncul sebagai akibat dari karakter lingkungan teknologi yang dinamis dan berkembang, dengan konsekuensi positif dan negatif bagi individu. Salah satu konsekuensi negatif dan aktivitas menyimpang yang mungkin diklasifikasikan sebagai elemen gelap dari komunikasi berbasis teknologi adalah *cyberstalking*[1].

*Cyberstalking* merupakan tindakan mengganggu atau melecehkan seseorang yang dilakukan dengan memanfaatkan kecanggihan teknologi. Dengan memanfaatkan kecanggihan teknologi pelaku *cyberstalking* memperoleh data diri korban yang kemudian data diri itu disalahgunakan untuk kepentingan pribadi pelaku. Sedangkan definisi *cyberstalking*, menurut *Black's Law Dictionary* edisi ke-9, adalah sebagai berikut:

> "*The act of threatening, harassing, or annoying someone via multiple e-mail messages sent over the internet, especially with the intent of instilling fear in the recipient that an illegal act or injury will be inflicted on the recipient, a member of the recipient's family or household.*"[2]
>
> "Mengancam, melecehkan, atau mencoba mengintimidasi seseorang melalui berbagai komunikasi, seperti melalui Internet, untuk menakut-nakuti penerima kejahatan kriminal atau tindakan yang dilakukan penerima atau kerabatnya."[3]

---

[1] Puneet Kaur, Amandeep Dhir, Anushree Tandon, Ebtesam A. Alzeiby, Abeer Ahmed Abohassan, (2021) A systematic literature review on cyberstalking. An analysis of past achievements and future promises, Technological Forecasting and Social Change, Volume 163, https://doi.org/10.1016/j.techfore.2020.120426.

[2] Ridho, M. F. (2020). *KEJAHATAN CYBERSTALKING DALAM PERSPEKTIF HUKUM POSITIF DAN HUKUM ISLAM (Analisis Kejahatan Cyberstalking Terhadap Gubernur DKI Jakarta Anies Rasyid Baswedan di Media Sosial) (Bachelor's thesis*, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta). hlm. 21

[3] Fadilah, Andi., Renda Aranggraeni., & Sri Reski Putri. (2021). Eksistensi Keamanan Siber terhadap Tindakan Cyberstalking dalam Sistem Pertanggungjawaban Pidana Cybercrime. Syntax *Literate: Jurnal Ilmiah Indonesia*. 6(4).hlm.1557

Tindakan *cyberstalking* dapat berpotensi menjadi suatu kejahatan apabila tidak ditangani secara mendalam. Pelaku *cyberstalking* menggunakan strategi dan teknik dalam mengancam, mempermalukan, mengintimidasi dan mengendalikan target mereka. Faktanya para pelaku *cyberstalking* paham akan teknologi serta memiliki banyak cara untuk menyiksa, melecehkan hingga melakukan pengancaman kepada targetnya. *Cyberstalking* berpotensi menimbulkan berbagai konsekuensi fisik dan emosional kepada korban secara online, tidak jarang korban yang menjadi target akan mengalami kemarahan, ketakutan, dan depresi yang berujung pada kematian.

Pelaku *cyberstalking* melancarkan aksinya melalui internet dengan memperoleh data pribadi korban melalui jejaring sosial media seperti memperoleh nama, alamat, latar belakang keluarga, nomor telepon, informasi rutin harian, tanggal lahir dan lain-lain. Setelah memperoleh data pribadi pelaku melakukan tindakan berupa melecehkan korban secara berulang seperti melakukan panggilan telepon dengan melecehkan atau meninggalkan pesan ancaman kepada korban yang dilakukan melalui layanan internet. Selain mengancam, pelaku dapat menyalahgunakan informasi atau data pribadi korban dengan mempostingnya pada situs web yang berhubungan dengan seks atau layanan kencan yang berpura-pura menjadi korban.

Pengertian *stalking* sendiri adalah mengikuti atau menguntit seseorang atau sesuatu karena obsesi. Ia lebih dari sekadar melacak atau meneror, mengirim pesan terus-menerus, menelepon, dan bahkan memantau kehidupan orang dengan cermat. Dalam dunia digital, ini disebut *cyberstalking*. Definisi lengkap *cyberstalking* adalah tindakan yang sama yang dilakukan melalui penggunaan internet atau metode digital lainnya untuk melecehkan individu, sekelompok individu, atau organisasi. Media internet yang digunakan dapat berupa media sosial, forum atau pesan elektronik *(e-mail).*

*Cybercrime* adalah kejahatan yang timbul karena kemajuan teknologi dan perkembangannya, serta cepatnya penyebaran informasi di Internet atau "dunia siber". Salah satu jenis kejahatan dunia maya adalah *cyberstalking*. Ada dua bentuk *cyberstalking*, *cyberstalking* sebagai tindakan tersendiri yaitu *stalking*, dan *cyberstalking* sebagai tindakan yang diikuti oleh tindakan lain termasuk mengancam, melecehkan, mengganggu seseorang, tuduhan palsu (fitnah), tindakan ini dilakukan melalui penggunaan alat elektronik, media elektronik, atau media internet, oleh orang yang tidak dikenal atau dikenal atau dikenal oleh korban. Peraturan perundang-undangan nasional Indonesia belum secara khusus mengatur perilaku pelacakan online. *Cyberstalking* sebagai tindakan tersendiri yaitu menguntit dan tindakan kriminal lainnya (yaitu pelecehan, pelecehan, pencemaran nama baik) juga telah diatur dalam hukum pidana, undang-undang ITE dan KUHP, jadi jika ada kasus *cyberstalking* di Indonesia nanti, tidak akan ada kekosongan hukum.

Umumnya, *cyberstalking* dianggap kejahatan hanya jika korban merasa terancam oleh *cyberstalking*. Hal ini diperjelas lebih lanjut dalam UU No. 1. Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang selanjutnya disebut UU ITE. Dalam UU ITE, *cyberstalking* dapat digolongkan sebagai perbuatan yang dilarang, sebagaimana diatur dalam Pasal 27 ayat 3 dan ayat 4 UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE):

*Ayat (3): "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Ayat (4): "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman".*

Berdasarkan UU ITE No 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008 menegaskan bahwa *cyberstalking* dapat dikategorikan sebagai tindak kejahatan apabila pelaku mengirimkan ancaman melalui jejaring internet terhadap korban. Sementara apabila pelaku hanya memantau korban saja maka hal terbsebut belum termasuk dalam tindak kejahatan. Kendatinya pelaku yang bersifat hanya memantau saja dapat menjadi langkah awal dalam melakukan kejahatan lainnya. Misalnya pelaku yang telah memiliki dendam pribadi terhadap korban sehingga pelaku itu memantau korban melalui jaringan internet yang kemudian dengan melakukan pemantauan itu maka pelaku mendapatkan identitas data pribadi korban berupa nama, nomor telepon, latar belakang keluarga hingga alamat rumah. Setelah menelusuri informasi yang didapatkan pelaku mulai menjalankan aksinya yaitu berupa melakukan pencurian, pembunuhan berencana hingga tindakan-tindakan yang merujuk pada kejahatan pidana lainnya. Contoh kasus *cyberstalking* dapat dibaca pada penelitian yang dilakukan oleh Juditha, dia meneliti tindakan *cyberstalking* di media sosial Twitter yang dilakukan oleh akun @TrioMacan2000 pada ajang pemilu tahun 2014. Kategori *cyberstalking* yang paling terlihat adalah keinginan untuk menyakiti, ketidakseimbangan kekuatan, pengulanan dan kesenangan yang dirasakan oleh pelaku[4].

Pemantauan informasi akan menyebabkan pelaku melakukan pengancaman hingga pemerasan terhadap korban sehingga membuat korban melaporkan tindakan itu kepada pihak yang berwenang. Setelah melaporkan pihak yang berwenang akan menjalankan penyelidikan hingga penyidikan atas kasus itu. Dalam menjalankan penyelidikan dan penyidikan tentunya terdapat beberapa hambatan yang akan menyulitkan penyidik dalam mendapatkan informasi maupun alat bukti seperti terhapusnya *sylog server* hingga dalam menetapkan tersangka.

Berdasarkan pembahasan diatas maka penulis menjabarkan rumusan permasalahan yang akan dibahas sebagai berikut: (1) Bagaimana Pengaturan hukum terhadap tindakan *cyberstalking* menggunakan akun palsu *(fake account)* yang merujuk pada tindak pidana? (2) Bagaimana proses penyidikan tindak kejahatan *cyberstalking* di Indonesia?

Tujuan dari artikel dengan judul "*Cyberstalking*: Kejahatan Dunia Maya terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana" ini adalah untuk memberikan pemahaman kepada masyarakat luas terkait penegakan hukum terhadap tindakan *cyberstalking* menggunakan akun palsu *(fake account)* yang merujuk pada tindak pidana dan untuk memberikan pemahaman terkait proses penyidikan tindak kejahatan *cyberstalking* di Indonesia.

[4] Juditha, C. (2015). Cyberstalking on Twitter@ triomacan2000 at Election 2014. *Jurnal Penelitian Komunikasi*, *18*(1).

Penelitian terkait *cyberstalking* telah dilakukan oleh banyak peneliti. Seperti Kaur *et al.* melakukan *systematic literature review* tentang *cyberstalking* lebih spesikfiknya, mereka menganalisis 50 penelitian yang telah ada terkait *cyberstalking* dan kerangka berpikir yang tepat secara teori dan metode untuk *cyberstalking*[5]. Ada pula yang menganailisis *cyberstalking* menggunakan pengguna jejaring sosial sebagai sampelnya. Penelitian mereka membahas tindakan pencegahan, karakteristik, dan dampak *cyberstalking* pada para korban[6]. Kemudian penelitian *cyberstalking* dari segi cara pendeteksiannya, penelitian ini merupakan analisis tekstual[7]. Selain mendeteksi *cyberstalking,* penelitian telah dilakukan dalam melakukan perlawanan pada *cyberstalking* yang dilakukan melalui *e-mail*[8]. Kemudian, pada tahun 2020 telah diterbitkan penelitian terkait *cyberstalking* dan penegakkan hukumnya[9].

## II. METODE PENELITIAN

Penelitian ini merupakan bagian dari penelitian hukum normatif dengan pendekatan perundang-undangan. Metode yang diadopsi dalam penelitian ini terkait *Cyberstalking:* Kejahatan Dunia Maya terhadap Perlindungan Data Pribadi Sebagai Pemicu Metodologi penelitian hukum normatif diperoleh dari sumber penelitian berupa dokumen hukum yang digunakan dalam studi kejahatan. Ada dua jenis sumber hukum yang digunakan dalam penelitian ini, yaitu bahan hukum primer dan bahan hukum sekunder. UU ITE No. 19 Tahun 2016, Perubahan atas UU ITE No. 11 Tahun 2008, dan KUHP digunakan sebagai sumber hukum utama (KUHP). Sementara itu, bahan sekunder hukum seperti buku, jurnal hukum, internet, dan pendapat ahli dikumpulkan melalui studi kepustakaan. Pengumpulan data dilakukan melalui metode dokumentasi Teknik analisis data yang digunakan dalam penelitian ini adalah teknik analisis kualitatif dimana penulis mendefinisikan dan menjelaskan masalah saat ini berdasarkan fakta-fakta tertentu yang muncul, yaitu fakta-fakta yang dapat dikonfirmasi secara ilmiah, dan kemudian menarik kesimpulan dari fakta-fakta tersebut. Informasi yang disajikan di sini adalah tentang kejahatan *cyberstalking*.

[5] Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426.

[6] Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking*, *17*(2), 61-67.

[7] Frommholz, I., Al-Khateeb, H. M., Potthast, M., Ghasem, Z., Shukla, M., & Short, E. (2016). On textual analysis and machine learning for cyberstalking detection. *Datenbank-Spektrum*, *16*(2), 127-135.

[8] Ghasem, Z., Frommholz, I., & Maple, C. (2015, July). A hybrid approach to combat email-based cyberstalking. In *2015 Fourth International Conference on Future Generation Communication Technology (FGCT)* (pp. 1-6). IEEE.

[9] Chang, W. J. (2020). Cyberstalking and law enforcement. *Procedia Computer Science*, *176*, 1188-1194.

## III. PEMBAHASAN

### Pengaturan Hukum Terhadap Tindakan *Cyberstalking* Menggunakan *Fake Account* Yang Merujuk Pada tindak pidana

Tindakan *cyberstalking* merupakan langkah awal terjadinya *cybercrime* dalam dunia maya. Tindakan *cyberstalking* dilakukan dengan melakukan pemantauan terhadap target guna memperoleh segala sumber informasi terkait data pribadi korban melalui kecanggihan teknologi. Umumnya pelaku menargetkan korban karena memiliki unsur kecemburuan ataupun dendam pribadi. Pelaku *cyberstalking* dalam hal menjalankan aksinya tidak melakukan pembuntutan terhadap korban secara langsung melainkan pelaku *cyberstalking* memperoleh data pribadi korban melalui jaringan sosial media yang kemudian data itu dipergunakan untuk suatu hal yang merugikan korban. Pelaku *cyberstalking* melancarkan aksinya melalui internet dengan memperoleh data pribadi korban melalui jejaring sosial media seperti memperoleh nama, alamat, latar belakang keluarga, nomor telepon, informasi rutin harian, tanggal lahir dan lain-lain. Setelah memperoleh data pribadi pelaku melakukan tindakan berupa melecehkan korban secara berulang seperti melakukan panggilan telepon dengan melecehkan atau meninggalkan pesan ancaman kepada korban yang dilakukan melalui layanan internet. Selain mengancam, pelaku dapat menyalahgunakan informasi atau data pribadi korban dengan mempostingnya pada situs web yang berhubungan dengan seks atau layanan kencan yang berpura-pura menjadi korban.

Dengan tidak adanya unsur seperti pelecehan atau pencemaran nama baik, pemerasan, ancaman, dan/atau ancaman kekerasan, *stalker* tidak dapat dihukum.[10] Apabila unsur-unsur itu terpenuhi maka hal itu merupakan Tindakan *cyberstalking* yang akan dituntut berdasarkan undang-undang yang berlaku. Peraturan yang dapat dijadikan sebagai landasan atas terjadinya kejahatan cyberstalking di Indonesia yaitu UU ITE No 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008. Peraturan itu merupakan peraturan yang mengatur tindak kejahatan yang dilakukan melalui jaringan teknologi dan internet. Pasal yang dapat dijadikan sebagai landasan yaitu pasal 27 ayat (3) dan ayat (4) *jo* pasal 45 ayat (1) UU ITE No 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008 sebagai berikut:

> *Pasal 27 Ayat (3): "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik".*
>
> *Pasal 27 Ayat (4): "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman".*
>
> *Pasal 45 Ayat (1): "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".*

Berkembangnya pola pikir manusia yang semakin maju, pelaku *cyberstalking* mulai menggerakkan aksinya dengan menggunakan akun palsu *(fake account)* untuk meminimalisir agar pelaku tidak dikenali oleh korban, hal itu akan berdampak pada

[10] Fadilah, Andi., Renda Aranggraeni., & Sri Reski Putri. (2021). *Ibid.* hlm. 1563

sulitnya aparat penegak hukum dalam mencari pelaku. Banyaknya pengguna sosial media yang membuat akun palsu disebabkan belum terdapatnya suatu sistem yang mendata pengguna internet yang memiliki kredibilitas, sehingga banyak bertebaran pengguna sosial media menggunakan identitas palsu. Apalagi hingga saat ini program media sosial belum menggunakan sistem verifikasi data yang transparan untuk memastikan keabsahan identitas pengguna pada saat pendaftaran.[11] Maka dari itu pengguna sosial media dengan menggunakan identitas akun palsu *(fake account)* sangat marak dijumpai.

Tujuan pelaku dalam hal membuat akun media sosial palsu yaitu sebagai sarana untuk menguntit, memata-matai maupun melakukan pemerasan kepada korban.[12] Penguntitan terhadap korban menggunakan akun palsu bertujuan memperoleh data pribadi tanpa diketahui dengan jelas siapa pelakunya. Pelaku yang menggunakan akun palsu *(fake account)* dalam menjalankan aksinya dapat dijerat pada UU ITE No 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008 pada pasal 35 *jo* pasal 51 ayat (1) sebagaimana penjelasan pasal itu menjelaskan bahwasanya seseorang yang dengan sengaja dan tidak memiliki hak atau melawan hukum dalam menipulasi membuat akun palsu *(fake account)* maka akan diancam pidana paling lama 12 (dua belas) tahun dan/atau denda maksimal Rp.12.000.000.000.- (dua belas milyar rupiah).[13]

Berkaitan dengan UU ITE pasal 35 pada kata "manipulasi" memiliki kesinambungan arti terhadap pelaku *cyberstalking* yaitu upaya dari sekelompok atau perseorangan untuk menyerang atau memengaruhi emosi dan mental orang lain, sehingga pelaku bisa mengendalikan korban dan mendapatkan apa yang pelaku inginkan. Korban akan diuntungkan dengan adanya putusan pengadilan terhadap pelaku kejahatan, tetapi pengadilan juga harus mempertimbangkan kerugian materil dan/atau immateriil korban. Dalam memperhatikan kerugian itu pengadilan juga harus menjatuhkan keputusan terhadap pelaku agar memberikan ganti kerugian atau restitusi yang diderita oleh korban secara materiil.[14]

Permohonan ganti rugi yang diajukan sebagai tanggapan atas putusan pengadilan bersifat permanen, yang mewajibkan pelaku untuk memberi ganti rugi kepada korban atas kerugian yang dideritanya. Korban dilindungi oleh klausul ganti rugi, yang memungkinkan korban diberi kompensasi atas kerugiannya. Mereka yang dirugikan sebagai akibat dari kegiatan melawan hukum orang lain berhak atas kompensasi, menurut Pasal 1365 KUH Perdata.[15] Tujuan dari kompensasi adalah untuk mengganti kerugian korban sementara juga menghalangi pelaku dengan membebankan harga untuk tindakan kriminal.

---

[11] Fadilah, Andi., Renda Aranggraeni., & Sri Reski Putri. (2021). *Ibid.* hlm.1559

[12] Haryanti, Syifa Devi Putri. (2021). "Apa Itu Cyber-Stalkers pada Media Sosial? Berikut Penjelasan Pakar untuk Hindari hal Itu." https://mediablitar.pikiran-rakyat.com/teknologi/pr-322432926/apa-itu-cyber-stalkers-pada-media-sosial-berikut-penjelasan-pakar-untuk-hindari-hal-itu?page=2&_gl=1*1dpd9zi*_ga*QWNQVXlzb2FjU09EaTBUNDZERGFZWERNY0cxemNxNnJwcXJmWERaT21vVGVlUXc0SjdWQVJCWWNZWjdsS0lucw, Diakses pada 7 Februari 2022

[13] Justika. "Hukum Membuat Fake Akun di Sosial Media Dengan Identitas Orang Lain". https://blog.justika.com/teknologi-informasi/hukum-membuat-fake-akun-di-sosial-media/. Dikutip pada 15 Februari 2022.

[14] Wijaya, Irawan Adi. (2018). Pemberian Restitusi Sebagai Perlindungan Hukum Korban Tindak Pidana. *Jurnal Hukum Dan Pembangunan Ekonomi.* 6(2). hlm.105

[15] Marasabessy, F. (2016). Restitusi Bagi Korban Tindak Pidana: Sebuah Tawaran Mekanisme Baru. *Jurnal Hukum & Pembangunan*, *45*(1), hlm.55

Pengaturan lain yang dapat dijadikan sebagai dasar hukum atas kejahatan *cyberstalking* yaitu pada pasal 310 ayat (1) dan (2) Kitab Undang-Undang Hukum Pidana (KUHP), dalam pasa; itu menerangkan sebagai berikut:[16]

> *Pasal 310 ayat 1: "Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah."*
>
> *Pasal 310 ayat 2: "Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah."*

Pada kutipan ayat pertama apabila dikaitkan dengan *cyberstalking* akan memiliki persamaan yang terletak pada kata "menyerang". Pelaku tindakan *cyberstalking* umumnya melakukan penyerangan berupa mencemarkan nama baik seseorang dengan mendapatkan informasi terkait data pribadi seseorang melalui kecanggihan teknologi. Perolehan data itu nantinya akan disebarluaskan kepada masyarakat umum. Data yang telah diperoleh oleh pelaku akan direkayasa menjadi berita yang menjelekkan hingga menjatuhkan kehormatan korban. Dengan dilakukan hal itu maka akan menimbulkan kerugian bagi korban. Akibatnya, pelanggar akan menghadapi hukuman hingga sembilan bulan penjara atau denda hingga Rp 4.500. Menurut kutipan kedua, jika seorang pelaku *cyberstalking* mencemarkan nama baik seseorang melalui teks atau mengirim foto, ia menghadapi hukuman maksimum satu tahun empat bulan penjara atau denda Rp 4.500.

Berdasarkan peraturan-peraturan yang telah penulis uraikan di atas, yang meliputi UU No. 1. Perubahan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Hukum Pidana (KUHP). Isu yang terdapat dalam *cyberstalking* akan lebih spesifik pada UU ITE karena pelaku *cyberstalking* menggunakan sarana teknis dalam melakukan tindakannya. UU ITE fokus mengatur tindak pidana di dunia siber agar UU ITE dapat memberikan kepastian hukum bagi korban untuk melakukan aktivitasnya di berbagai sistem elektronik. Menurut ketentuan UU ITE saat ini mengarah pada ketentuan umum, namun cukup komprehensif, mencakup segala hal yang berkaitan dengan dunia *online*. UU ITE memuat konten baru dengan tema-tema seperti identifikasi transaksi dan bukti elektronik, penyelesaian sengketa, perlindungan data, nama domain dan hak kekayaan intelektual, serta bentuk-bentuk kegiatan terlarang dan sanksi yang belum pernah dipertimbangkan sebelumnya.[17]

---

[16] Ridho, M. F. (2020). *KEJAHATAN CYBERSTALKING DALAM PERSPEKTIF HUKUM POSITIF DAN HUKUM ISLAM (Analisis Kejahatan Cyberstalking Terhadap Gubernur DKI Jakarta Anies Rasyid Baswedan di Media Sosial), Op. Cit.* hlm.55

[17] Ramli, A. M. (2018). Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional. *Jurnal Legislasi Indonesia*, *5*(4), hlm.5

## Proses Penyidikan Tindak Kejahatan *Cyberstalking* di Indonesia

Kecanggihan teknologi yang semakin pesat dan kemajuan internet yang meningkat memunculkan masyarakat maya melalui perangkat komputer hingga *smartphone*. Kehadiran masyarakat maya semakin berkembang setiap tahunnya sehingga tak jarang terdapat suatu konflik atau permasalahan yang dapat merugikan salah satu pihak seperti penguntitan atau *cyberstalking* yang menjalankan aksinya dengan mengancam, mempermalukan, mengintimidasi dan mengendalikan target mereka melalui kecanggihan teknologi dan jaringan internet.

Target atau korban yang merasakan keresahan maupun ketakutan akan melaporkan pelaku kepada aparat penegak hukum terlebih dahulu dikarenakan tindakan *cyberstalking* termasuk kedalam delik aduan yang mana harus terdapat suatu pengaduan dari korban maka setelah itu aparat penegak hukum akan melakukan penyidikan dan penyelidikan atas kasus itu.[18] Aparat Kepolisian Negara Republik Indonesia atau Pejabat Pelayanan Publik Kementerian Komunikasi dan Informatika ("PPNS") berwenang menangani kejahatan dunia maya.

Polisi Kominfo atau PPNS akan melakukan penyidikan dan penyidikan, dan penulis akan memberikan pemahaman terlebih dahulu mengenai perbedaan penyidikan dan penyidikan sebelum memaparkan proses penyidikan dan penyidikan yang dilakukan oleh Polri atau PPNS Kementerian Komunikasi dan Informatika. Penyidikan adalah suatu tahapan untuk menemukan dan mengungkap suatu peristiwa dugaan tindak pidana, sedangkan penyidikan lebih menitikberatkan pada pencarian barang bukti sehingga tersangka dapat dikatakan telah melakukan tindak pidana.[19]

Proses penyidikan dimulai dengan laporan korban ke pihak yang berwenang, seperti polisi atau PPNS Kementerian Komunikasi dan Informatika. Setelah menerima laporan kasus korban oleh Polisi atau PPNS Kementerian Komunikasi dan Informatika, Polri atau PPNS Kementerian Komunikasi dan Informatika akan menghubungi pihak manapun yang dicurigai sebagai tersangka atau saksi untuk menanyakannya dan memverifikasi apakah salah satu pihak telah melakukan tindak pidana yang melibatkan transaksi teknologi informasi dan komunikasi. Polisi Kementerian Komunikasi dan Informatika atau PPNS juga melakukan penggeledahan yang diduga sebagai lokasi terjadinya tindak pidana illegal yang melibatkan transaksi teknologi informasi dan komunikasi. Penggeledahan dan/atau penyitaan sistem komputer yang terkait dengan dugaan tindak pidana harus dilakukan dengan persetujuan Ketua Pengadilan Negeri, sesuai dengan Pasal 43(3) UU ITE.[20] Polisi atau PPNS Kementerian Komunikasi dan Informatika melakukan tahap selanjutnya, yaitu tahap penyidikan, setelah menerima informasi bahwa telah terjadi sejumlah pelanggaran.

---

[18] Tampubolon, Musa Hengky P., Mulyati Pawennei & Zainuddin. (2021). Efektivitas Penyidikan Tindak Pidana Penipuan Secara Online. *Jurnal of Lex Generalis (JLS)*. 2(4). Hlm 15888-1589

[19]Kompas.com. (2021) "Perbedaan Penyelidikan dan Penyidikan" https://www.kompas.com/skola/read/2021/07/01/132727869/perbedaan-penyelidikan-dan-penyidikan. Dikutip pada 17 Februari 2022

[20] TAHIR, H. (2016). Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Tomalebbi*, (2), hlm.100-101.

Tahapan penyidikan diawali dengan penerbitan SPDP (Surat Perintah Dimulainya Penyidikan) dengan terbitnya surat SPDP memberikan tanda kepada penyidik untuk mengumpulkan bukti. Bukti yang harus dikumpulkan sekurang-kurangnya dua bukti sehingga dapat menetapkan seseorang menjadi tersangka.[21] Setelah memperoleh bukti penyidik melakukan pemanggilan saksi-saksi untuk menggali lebih dalam agar saksi itu dapat dijadikan sebagai bukti tambahan dan dapat memberikan pertimbangan dalam penyidikan pada kasus tindakan *cyberstalking*.

Setelah pemanggilan saksi, PPNS Kementerian Komunikasi dan Informatika melakukan gelar perkara yang bertujuan memaparkan tindakan-tindakan yang telah terlaksana pada proses penyidikan guna dapat merangkum kesimpulan atas penyelidikan itu. Setelah mendapatkan kesimpulan dan menyatakan bahwa terlapor yang diduga sebagai pelaku *cyberstalking* dinyatakan bersalah maka status terlapor berubah menjadi tersangka. Setelah penetapan tersangka maka akan dilakukan penagkapan dan penahanan, pembuatan berita acara pemeriksaan tersangka, penyitaan dan yang terakhir yaitu menyerahkan berkas perkara pada Jaksa Penuntut Umum (JPU). Pada tahap terakhir apabila Jaksa Penuntut Umum (JPU) menyatakan bahwa berkas yang diperoleh lengkap dan cukup maka akan masuk pada tahap penuntutan.

Pada tahap penyelidikan dan penyidikan pada tindak kejahatan *cyberstalking* tidak jauh beda dengan tahap penyelidikan dan penyidikan pada tindak kejahatan konvensional, yang menjadi perbedaan terletak pada pemeriksaan alat bukti. Pada kejahatan *cyberstalking* pemeriksaan barang bukti diperoleh dari data-data yang berada pada teknologi informasi seperti pada *sylog server*. *Sylog server* merupakan server penyimpan data *syslog* diberbagai macam komputer dan jaringan secara berpusat.[22] Apabila korban lambat dalam melakukan pelaporan kepada pihak kepolisian, maka pelaku dapat saja menghapus data-data serangan di sy*log server*. Terhapusnya *sylog server* akan menyulitkan penyidik dalam menemukan log statistik yang terdapat dalam server. Hal itulah yang menjadi penyebab sulitnya pihak kepolisian dalam menemukan bukti. Dalam kasus pelaku *cyberstalking* yang menggunakan akun palsu *(fake account)* peranan *sylog server* sangat dibutuhkan dikarenakan jika terdapatnya data statistik itu maka penyidik dapat mengetahui asal muasal pelaku *cyberstalking* yang menggunakan akun palsu *(fake account)*.[23]

Selain sulitnya mendapatkan bukti jika *sylog server*[24] terhapus terdapat juga beberapa kendala yang menyebabkan sulitnya penyidik memperoleh alat bukti yaitu berupa penetapan tersangka. Dengan hanya mendapatkan informasi dari korban berupa alamat sosial media maupun nomor telepon yang dimiliki pelaku maka hal itu belum dapat menjadi jaminan bahwa alamat sosial media maupun nomor telepon itu merupakan milik

---

[21] Rumondor, R. (2015). Alat Bukti Dan Pembuktian Tindak Pidana Informasi Teknologi Dan Transaksi Elektronik. *Lex Crimen*, *4*(4). hlm.140

[22] Ditanaya, T. H. (2016). *Rancang Bangun Sistem Log Server Berbasis Syslog dan Cassandra untuk Monitoring Pengelolaan Jaringan di ITS* (Doctoral dissertation, Institut Teknologi Sepuluh Nopember Surabaya). hlm.1

[23] Agus, A. A., & Riskawati, R. (2016). Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya*, *11*(1). hlm.50

[24] Server syslog adalah server yang menyimpan data syslog untuk berbagai perangkat komputer dan jaringan secara terpusat. Server syslog harus memiliki ketersediaan tinggi untuk melayani penyimpanan syslog setiap komputer dan perangkat jaringan

tersangka bisa saja tersangka melakukan penyamaran nama pada alamat sosial media ataupun menggunakan nomor telepon yang belum dilakukan registrasi. Untuk itu pihak kepolisian atau PPNS Kementerian Komunikasi dan Informatika selauku penegak hukum harus sangat ekstra dalam melakukan penyidikan pelaku *cyberstalking*.[25]

Penegakan hukum sangat memiliki peranan penting dalam mewujudkan ketertiban dan ketentraman masyarakat.[26] Peranan penyidik dalam melakukan penyidikan dalam menegakkan suatu keadilan bergantung pada kuantitas dan kualitas dari anggotanya. Dilihat berdasarkan kualitas pada pihak kepolisian, pihak kepolisian dalam melakukan penyidikan terhadap tindakan *cyber* wajib memahami seluk beluk teknologi.[27] Untuk menangani *cyberstalker*, polisi harus membentuk unit khusus, dengan masing-masing anggota di bidang informasi dan transaksi elektronik mampu mendeteksi *cybercrime*.

Pengungkapan kasus *cyberstalking* tidak hanya membutuhkan keterampilan dari pihak kepolisian dalam memahami teknologi melainkan juga membutuhkan fasilitas yang mampu menunjang kinerja dari pihak kepolisian. Fasilitas yang dibutuhkan oleh pihak kepolisian ialah berupa laboratorium forensik komputer. Tersedianya fasilitas tersebut memungkinkan pengungkapan barang bukti berupa data digital dengan cara merekam dan menyimpan barang bukti berupa gambar, program, html, suara, dan lain-lain dalam bentuk *soft copy*. Forensik komputer adalah cabang kedua dari ilmu forensik, berkaitan dengan bukti hukum yang ditemukan di komputer dan perangkat penyimpanan digital lainnya.[28] Forensik komputer, juga dikenal sebagai digitale Forensik, bertujuan untuk memberikan keamanan dengan menganalisis bukti digital dan memperoleh fakta objektif tentang insiden atau pelanggaran keamanan dalam sistem informasi. Fakta-fakta ini akan digunakan sebagai bukti di ruang sidang. Misalnya, kita dapat menggunakan Forensik Internet untuk menentukan siapa, kapan, dan di mana email dikirimkan kepada kita. Dalam contoh lain, kita dapat melihat informasi alamat IP lengkap pengunjung situs web, komputer yang mereka gunakan, keberadaan dan aktivitas mereka di situs web kami.[29]

Sarana dan prasarana harus memadai berdasarkan kerangka penegakan hukum, hukum seringkali sulit ditegakkan karena fasilitas yang tidak memadai atau tidak ada. Karena kurangnya sarana dan prasarana pendukung, menyebabkan terhambatnya kinerja dari aparat penegakan hukum sehingga aparat penegak hukum tidak akan bisa memainkan perannya yang sebenarnya. Tersedianya sarana dan prasarana yang memadai mampu meningkatkan aparat penegak hukum dalam memperoleh kepastian hingga kecepatan dalam menyelesaikan suatu perkara. Jika tingkat keamanan dan kecepatan pemrosesan

[25]Agus, A. A., & Riskawati, R. (2016). *Ibid*.hlm.100

[26] Ariyanti, V. (2019). Kebijakan Penegakan Hukum Dalam Sistem Peradilan Pidana Indonesia. *Jurnal Yuridis*, *6*(2), 33-54.

[27]Nurlaela, siti. (2020). Peran Dan Tanggung Jawab Kepolisian Negara Republik Indonesia Daerah Jawa Barat Dalam Penegakan Hukum Tindak Pidana Siber Dikaitkan Dengan Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Dan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Elibrary UNIKOM*.hlm.57

[28] Safitri, D. E. (2020). Penegakan Hukum terhadap Pelaku Perjudian Online di Kota Makassar. *Jurnal Magister Hukum ARGUMENTUM*, *7*(1), 10-15.

[29] Agis, Abdul. "Peranan Kepolisian dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronika (Ite)." *Al Hikam*, *1*(2),. hlm. 53-54

kasus ditingkatkan, maka penerapan hukuman-hukuman yang dibentuk akan memiliki efek yang menakutkan sehingga meminimalisir pelaku tindak kejahatan.[30]

Pencegahan kejahatan tidak akan berhasil jika hanya mengandalkan aparat penegak hukum saja melainkan harus memerlukan peran dari setiap individu masyarakat. Setiap individu wajib diberikan edukasi terkait tidak melibatkan dirinya menjadi pelaku maupun korban kejahatan *cyberstalking*. Setiap individu akan menuntut suatu keadilan, tetapi individu itu harus menjadikan dirinya sebagai anggota masyarakat yang sadar akan hukum beserta meningkatkan solidaritas antar sesama individu.[31] Setiap individu juga berperan penting dalam menciptakan lingkungan yang kondusif serta memiliki kepedulian tinggi terhadap individu lainnya.

## IV. KESIMPULAN

Berdasarkan hasil pembahasaan dalam penelitian itu, maka penulis menarik kesimpulan bahwasanya atas berkembangnya teknologi yang begitu pesat banyak memunculkan kejahatan-kejahatan yang bersumber pada kecanggihan teknologi diantaranya terkait tindakan *cyberstalking*, sehingga memerlukan suatu peraturan khusus yang mengatur tindakan *cyberstalking*. Dengan demikian, dalam menangani problematika terkait pengaturan tindak kejahatan *cyberstalking,* maka diperlukanlah suatu pengaturan pidana dengan menegaskan "barangsiapa" dengan sengaja melakukan penguntitan terhadap orang lain melalui sarana media internet, dengan mengirimkan informasi elektronik secara pribadi kepada orang lain, dan tindakannya menimbulkan gangguan terhadap diri orang lain itu, diancam dengan ancaman pidana. Namun, tindakan *cyberstalking* perlu dikriminalisasi dengan batas-batas yang jelas, yaitu dengan mengkualifikasikannya sebagai delik aduan, dan dalam penjatuhan sanksi, penegak hukum harus memperhatikan kondisi kejiwaan dari pelaku. Atau dengan kata lain, pemerintah dapat mengatur dan mengesahkan RUU terkait perlindungan data pribadi yang mana sangatlah penting dilakukan di era digital ini.

Dalam hal penegakan hukum, lembaga penegak hukum harus membentuk unit khusus untuk menangani kasus *cyberstalking*. Anggota entitas harus memiliki pengetahuan di bidang informasi dan transaksi elektronik, serta harus menyediakan fasilitas yang memadai untuk pelaksanaan tugasnya, seperti menyediakan laboratorium forensik komputer untuk pengungkapan data dan catatan digital serta penyimpanan barang bukti.

[30] Windari, R. A. (2011). Penegakan Hukum Terhadap Perlindungan Anak Di Indonesia (Kajian Normatif Atas Bekerjanya Hukum Dalam Masyarakat). *Media Komunikasi FPIPS*, *10*(1).

[31] Panjaitan, P. I. (2018). USAHA MASYARAKAT MENCEGAH KEJAHATAN. *to-ra*, *4*(1),hlm.25

## DAFTAR PUSTAKA


Agis, Abdul. "Peranan Kepolisian dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronika (Ite)." *Al Hikam,* 1(2).

Agus, A. A., & Riskawati, R. (2016). Penanganan Kasus *Cyber Crime* Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya,* 11(1).

Azhari, Muhammad Redha. (2019). Aspek Pidana Mayantara (*Cyberstalking*). *Badamai Law Journal*, 4(1).

Ariyanti, V. (2019). Kebijakan Penegakan Hukum Dalam Sistem Peradilan Pidana Indonesia. *Jurnal Yuridis*, 6(2), 33-54.

Ditanaya, T. H. (2016). Rancang Bangun Sistem Log Server Berbasis Syslog dan Cassandra untuk Monitoring Pengelolaan Jaringan di ITS *(Doctoral dissertation, Institut Teknologi Sepuluh Nopember Surabaya).*

Fadilah, Andi., Renda Aranggraeni., & Sri Reski Putri. (2021). Eksistensi Keamanan Siber terhadap Tindakan Cyberstalking dalam Sistem Pertanggungjawaban Pidana Cybercrime. *Syntax Literate:Jurnal Ilmiah Indonesia*. 6(4).

Haryanti, Syifa Devi Putri. (2021). "Apa Itu Cyber-Stalkers pada Media Sosial? Berikut Penjelasan Pakar untuk Hindari hal Itu." https://mediablitar.pikiran-rakyat.com/teknologi/pr-322432926/apa-itu-cyber-stalkers-pada-media-sosial-berikut-penjelasan-pakar-untuk-hindari-hal-itu?page=2&_gl=1*1dpd9zi*_ga*QWNQVXlzb2FjU09EaTBUNDZERGFZWERNY0cxemNxNnJwcXJmWERaT21vVGVlUXc0SjdWQVJCWWNZWjdsS0lucw, Diakses pada 7 Februari 2022

Imron, Ali., Muhamad Iqbal. (2019) Hukum Pembuktian. *Tanggerang Selatan: UNPAM PRESS*

Justika. "Hukum Membuat Fake Akun di Sosial Media Dengan Identitas Orang Lain". https://blog.justika.com/teknologi-informasi/hukum-membuat-fake-akun-di-sosial-media/. Dikutip pada 15 Februari 2022.

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, 163, https://doi.org/10.1016/j.techfore.2020.120426.

Kompas.com. (2021) "Perbedaan Penyelidikan dan Penyidikan" https://www.kompas.com/skola/read/2021/07/01/132727869/perbedaan-penyelidikan-dan-penyidikan. Dikutip pada 17 Februari 2022

Marasabessy, F. (2016). Restitusi Bagi Korban Tindak Pidana: Sebuah Tawaran Mekanisme Baru. *Jurnal Hukum & Pembangunan*, 45(1), hlm.55

Nurlaela, siti. (2020). Peran Dan Tanggung Jawab Kepolisian Negara Republik Indonesia Daerah Jawa Barat Dalam Penegakan Hukum Tindak Pidana Siber Dikaitkan Dengan Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Dan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Elibrary UNIKOM.*

Panjaitan, P. I. (2018). USAHA MASYARAKAT MENCEGAH KEJAHATAN. *to-ra*, *4*(1)

Ramli, A. M. (2018). Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional. *Jurnal Legislasi Indonesia*, *5*(4).

Ridho, M. F. (2020). KEJAHATAN CYBERSTALKING DALAM PERSPEKTIF HUKUM POSITIF DAN HUKUM ISLAM (Analisis Kejahatan Cyberstalking Terhadap Gubernur DKI Jakarta Anies Rasyid Baswedan di Media Sosial) *(Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta).*

Rumondor, R. (2015). Alat Bukti Dan Pembuktian Tindak Pidana Informasi Teknologi Dan Transaksi Elektronik. *Lex Crimen*, 4(4).

Safitri, D. E. (2020). Penegakan Hukum terhadap Pelaku Perjudian Online di Kota Makassar. *Jurnal Magister Hukum ARGUMENTUM,* 7(1), 10-15.

TAHIR, H. (2016). Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Tomalebb.*, (2).

Tampubolon, Musa Hengky P., Mulyati Pawennei & Zainuddin. (2021). Efektivitas Penyidikan Tindak Pidana Penipuan Secara Online. *Jurnal of Lex Generalis (JLS).* 2(4).

Wijaya, Irawan Adi. (2018). Pemberian Restitusi Sebagai Perlindungan Hukum Korban Tindak Pidana. *Jurnal Hukum Dan Pembangunan Ekonomi*. 6(2).

Windari, R. A. (2011). Penegakan Hukum Terhadap Perlindungan Anak Di Indonesia (Kajian Normatif Atas Bekerjanya Hukum Dalam Masyarakat). *Media Komunikasi FPIPS*.