(2024), 2 (1): 236–344 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN IDENTITAS ONLINE DI INDONESIA

Khadafi Yusuf [1)], M Frasetyo [2)], Reza Ramdan Gumilar [3)], Asmak Ul Hosnah[,4)].

Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia [1234]

Alamat e-mail : khadafidxo46@gmail.com [1], muhamadfrasetyo506@gmail.com [2], sintiadewihantika@gmail.com [3], asmak.hosnah@unpak.ac.id [4]

Correspondence
Email: No. Telp:
Submitted 6 januari 2024 Accepted 12 januari 2024 Published 13 januari 2024

ABSTRACT

Cyberstalking is the act of harassing or demeaning someone by utilizing moderntechnology. Through this technology, cyberstalkers can access the victim's personal dataand misuse it for their own personal gain. It often involves taking and exploitingthevictim's personal data to harm or harass them online. This includes actions suchassending threats, demeaning the victim, pursuing them online, or even disseminatingfalseor personal information about the victim with the intention of damaging their reputation. The impact of cyberstalking can be very serious on the physical and mental well-beingof victims, and often requires legal action to protect them and uphold their right to privacy. This research is focused on applying a normative legal approach and analytical descriptiveresearch, in the discussion process, the data is presented comprehensively, in detail, andstructured, and then analyzed by referring to the theoretical framework in legal scienceandapplicable regulations. The data collection method used is the literature study method. The results of this research are expected to provide a deeper understanding of theknowledge of legal protection for victims of online identity crimes in Indonesia

Keyword : *Cyberstalking, False Information, Personal Data*

ABSTRAK

Cyberstalking adalah tindakan mengganggu atau merendahkan seseorang denganmemanfaatkan teknologi modern. Melalui teknologi ini, pelaku cyberstalking dapat mengakses data pribadi korban dan menyalahgunakannya untuk kepentingan pribadi mereka sendiri. Tindakan ini sering melibatkan pengambilan dan eksploitasi data pribadi korban untuk merugikan atau mengganggu mereka di dunia maya. Ini mencakup tindakanseperti mengirim ancaman, merendahkan korban, mengejar mereka secara online, ataubahkan menyebarluaskan informasi palsu atau pribadi korban dengan niat merusakreputasi mereka. Dampak dari cyberstalking dapat sangat serius terhadap kesejahteraan fisik dan mental korban, dan seringkali memerlukan tindakan hukumuntuk melindungi mereka dan menegakkan hak privasi mereka. Penelitian ini difokuskan menerapkanpendekatan hukum normatif serta penelitian bersifat deskriptif analitis, dalamprosespembahasan, data disajikan secara komprehensif, mendetail, dan terstruktur, dankemudian dianalisis dengan mengacu pada kerangka teori dalamilmu hukumdanperaturan yang tengah diberlakukan. Untuk mengumpulkan berbagai data dipakai sebuahmetode yang berupa metode studi kepustakaan. Melalui dihasilkannya penelitianini dimiliki sebuah harapan agar bisa menyampaikan pemahaman dengan penelitianini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai pengetahuanperlindungan hukum terhadap korban kejahatan identitas online di Indonesia.

Kata kunci: Cyberstalking, Informasi Palsu, Data Pribadi

Pendahuluan

Indonesia termasuk dalam negara yang tengah menjalani pertumbuhan, dan salah satu tanda perkembangan tersebut adalah melalui sejumlahbesar inisiatif pembangunan di

berbagai sektor kehidupan dalamkonteks bernegaradan bermasyarakat, termasuk perkembangan di sektor teknologi dantelekomunikasi. Bahkan, seiring dengan perkembangan tersebut, kesadaranmasyarakat untuk meningkatkan pemanfaatan teknologi yang mudahdigunakan semakin meningkat. Dalam era ini, memungkinkan segala hal untukdikelola dari berbagai lokasi menggunakan internet dan perangkat elektronikyang terkoneksi. Dampak dari perkembangan ini sangat pentingketikateknologi yang berfokus pada digital diadopsi digunakan oleh individudalamkegiatan sehari-hari seperti meningkatkan produktivitas kerja, memperkuat hubungan sosial dan ekonomi, serta memberikan kemudahan dalamberagamaspek.[1]

Dengan kemajuan teknologi dan pertumbuhan informasi, disrupsi atautransformasi yang signifikan terus berlangsung di berbagai sektor. Saat ini, pemanfaatan teknologi semakin meluas, dan masyarakat tidak bisa menghindar dari keterlibatan dalam teknologi dalam kehidupan sehari-hari mereka.Cara hidup manusia telah diubah dan berkembang menjadi gayahidupyang berbeda melalui dampak globalisasi dengan pemakaian teknologi informasi beserta pemakaian komunikasi. Selain itu, hal ini juga mendorongterjadinya transformasi dalam bidang aspek sosial, budaya, pertahanan, keamanan, lalu bidang penegakan hukum, juga pastinya, pada sektor ekonomi. Pertumbuhan serta majunya teknologi informasi dengan sangat cepat termasuk dalam hal yang menyebabkanperubahan dalam aktivitas seseorang pada segala sektor yangmanadampaknya secara langsung sudah memengaruhi timbulnya jenis tindakanhukum yang baru.[2] Privasi memiliki signifikansi besar bagi individu karena pada hakikatnyasetiap orang memiliki aspek dari diri mereka yang ingin dijaga dari pengetahuanorang lain. Sebagai hasilnya, individu cenderung memiliki doronganuntukmenjaga kerahasiaan pribadi mereka, karena keinginan untuk melindungi privasi adalah hal yang berlaku secara universal untuk semua orang.

Perlindungan data pribadi adalah respons terhadap salahsatutantangan dalam menjaga hak privasi individu. Sama seperti yangtelahdisebutkan sebelumnya, elemen penting dari hak privasi adalah data pribadi. Oleh karena itu, hak privasi tidak selalu terbatas pada data pribadi, melainkandata pribadi adalah komponen yang menyusun hak privasi. Jika konsepperlindungan data pribadi menjadi fokus perhatian, maka akan terdapat keterkaitan dengan pelaksanaan hak privasi. Bermula dari dasar mengenai alasannya, rencana perlindungan, hingga penerapannya, pembahasanmengenai konsep adalah uraian yang sistematis dan pokok, yangdalam konteks ini membahas apa yang dimaksud dengan perlindungan yang berfokuspada data pribadi.[3]

Dampak dari perkembangan teknologi dan informasi ini tidak hanyadirasakan sebagai manfaat positif. Kemajuan teknologi komputer dantelekomunikasi, khususnya melalui media internet, sebagai sarana penyebaraninformasi dalam kehidupan sehari-hari, juga menghadirkan dampak negatif berupa penyalahgunaan seperti munculnya kejahatan di dunia maya(cybercrime). Salah satu dampak buruk dari perilaku menyimpang yangbisadianggap sebagai aspek yang gelap dalam komunikasi yang berdasarkanteknologi

[1] Sri Adiningsih, Transformasi Ekonomi Berbasis Digital di Indonesia, (Jakarta: GramediaPustaka Utama, 2019), hlm. 58.
[2] Siswanto Sunarso, Hukum Informasi dan Transaksi Elektronik, (Jakarta: Rineka Cipta, 2009), hlm. 5
[3] "Halaman Utama Dema Justicia Fakultas Hukum Universitas Gadjah Mada," DemaJusticia Fakultas Hukum Universitas Gadjah Mada, tersedia di: https://demajusticia.org/, diakses3November 2023.

yaitu berupa cyberstalking. Cyberstalking termasuk kedalamaksi mengganggu maupun menganggap rendah individu lewat pemanfaatanteknologi modern. Melalui teknologi ini, pelaku cyberstalking dapat mengaksesdata pribadi korban dan menyalahgunakannya untuk kepentingan pribadi mereka sendiri. Menurut International Journal of Cyber Criminology, cyberstalkingadalah suatu kegiatan seseorang yang menggunakan internet sebagai senajataatau alat yang digunakan untuk mengganggu/mengusik, mengancam, danmenimbulkan ketakutan.[4] Tindakan ini sering melibatkan pengambilandaneksploitasi data pribadi korban untuk merugikan atau mengganggu merekadi dunia maya. Ini mencakup tindakan seperti mengirim ancaman, merendahkankorban, mengejar mereka secara online, atau bahkan menyebarluaskaninformasi palsu atau pribadi korban dengan niat merusak reputasi mereka. Dampak dari cyberstalking dapat sangat serius terhadap kesejahteraanfisikdan mental korban, dan seringkali memerlukan tindakan hukumuntukmelindungi mereka dan menegakkan hak privasi mereka.

Tindakan cyberstalking dapat menjadi suatu tindak kejahatan seriusbilatidak diatasi dengan tegas. Strategi dan teknik tertentu digunakan olehpelakucyberstalking untuk mengancam, merendahkan, mengintimidasi, sertamengendalikan korban mereka. Pemahaman yang mendalamtentang teknologi dan berbagai cara untuk menyiksa, merendahkan, bahkan mengancamkorbanmereka dimiliki oleh mereka. Kesejahteraan fisik dan emosional korban secara online dapat seriusterpengaruh oleh cyberstalking. Tidak jarang, kemarahan, ketakutan, dandepresi dialami oleh korban, bahkan hingga berakhir dalamtragedi kematian. Setiap orang yang menjadi pelaku cyberstalking melakukan operasinyalewat internet melalui cara memantau dan mengumpulkan informasi pribadi korban, termasuk nama, alamat, riwayat keluarga, rutinitas sehari-hari, nomor telepon, hingga ke tanggal lahir juga lainnya, yang mereka peroleh melalui jejaring sosial media. Setelah mendapatkan informasi ini, pelaku melakukantindakan panggilan telepon yang dilakukan berulang dengan maksudpesanancaman atau pelecehan ditinggalkan kepada korban melalui layanan internet. Selain itu, pelaku juga dapat mengeksploitasi mengumpulkan dan memanipulasi informasi ataudatapribadi korban cara mempublikasikannya di situs web yang terkait denganhal- hal seksual yang berpura-pura menjadi korban. Cyberstalking sering kali hanya dianggap ilegal jika korbannya merasaterancam. Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentangInformasi dan Transaksi Elektronik (UU ITE) jo. Undang-Undang Nomor 1Tahun2016 tentang Informasi dan Transaksi Elektronik (UU ITE) semakinmenegaskan hal tersebut. Sesuai Undang-Undang Nomor 19 Tahun2016tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 27 ayat (3) dan(4) yang berbunyi sebagai berikut yang menerangkan cyberstalking dilarangdalamUU ITE:

Ayat (3): “Setiap Orang dengan sengaja dan tanpahakmendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronikyang memiliki muatan penghinaan dan/atau pencemaran nama baik”.

Ayat (4): “Setiap Orang dengan sengaja dan tanpahakmendistribusikan dan/atau

[4] Michael L. Pittaro, “Cyberstalking: An Analysis of Online Harassment and Intimidation”, International Journal of Cyber Criminology, (Vol. 1 No. 2 Tahun 2007) : 180.

mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronikyang memiliki muatan pemerasan dan/atau pengancaman".

Berlandaskan atas UU ITE yaitu dengan No 19 Tahun 2016, perubahandari UU ITE No 11 Tahun 2008, menerangkan jika tindakan kejahatanbisadikenakan pada kasus cyberstalking ketika pelaku mengirimkan ancamankepada korban melalui jaringan internet. Namun, jika pelaku hanya memantaukorban tanpa mengancam, tindakan tersebut belumdianggap sebagai kejahatan. Meskipun demikian, perlu dicatat bahwa pelaku yanghanyamelakukan pemantauan saja kemudian bisa mengambil tindakan permulaanuntuk menjalankan tindakan kejahatan lain. Sebagai contoh, pemantauankorban melalui internet dapat dimulai oleh pelaku yang merasa dendamterhadap korban, dan dari pemantauan tersebut mereka dapat memperolehinformasi pribadi korbannya, misalnya semacam nama, lalu hingga telepon, laluriwayat keluarganya, beserta alamat rumah. Perlindungan data pribadi telah menjadi isu yang semakin diperhatikanakhir-akhir ini. Peningkatan penggunaan platform digital merupakan salahsatuargumen mengapa keamanan data pribadi menjadi sangat esensial adalahuntuk melindungi integritas data pribadi. Oleh karena itu, dilandaskanpadapenjabaran tadi, fokus dalam jalannya penelitian yaitu mengkaji pentingnyaregulasi perlindungan data pribadi dianalisis sebagai bagian dari upayamemastikan keamanan data pribadi dalam rangka memenuhi hak privasi masyarakat Indonesia. Perlindungan informasi individu mencerminkan pengakuandankeamanan hak-hak dasar manusia yang esensial sesuai standar yang terkandung dalam Pancasila. Berbagai nilai Pancasila disini yakni berupasegala nilai kemanusiaan dan keadilan. Dari sudut pandang kemanusiaan, kitadiharapkan untuk bersikap manusiawi juga dengan tidak menggunakansuatudata yang bukan milik sendiri tanpa izin mereka, sementara dari sudut pandangkeadilan, kita diharapkan untuk memenuhi kewajiban kita sendiri danmenghormati hak privasi orang lain tanpa mengganggunya.[5] Dengan merujuk pada informasi yang disampaikan dalampengantar mengenai pentingnya perlindungan data pribadi, oleh karena itu, penyusunmerasa tertarik untuk melakukan penelitian tentang kejahatan identitas onlineyang dilakukan di Indonesia dengan judul: "Perlindungan HukumTerhadapKorban Kejahatan Identitas Online di Indonesia". Kemudian, rumusan masalahdari penelitian ini ialah akan membahas bagaimana pengaturan mengenai kejahatan identitas yang merusak data pribadi suatu individu.

Metode Penelitian

Definisi atas penelitian yaitu suatu aktivitas ilmiah dengan berlandaskankepada metode, struktur, beserta suatu pemikiran khusus dengan maksudagar bisa mengkaji satu ataupun sebagian dari fenomena hukum.[6] Padaberlangsungnya penelitian ini, penyusun menerapkan jenis penelitian kualitatif dengan menerapkan pendekatan hukum normatif, yaitu penelitian hukumdilakukan dengan mengkaji bahan pustaka atau data sekunder.[7]

[5] Erlina Maria Christin Sinaga dan Mery Christian Putri, "Formulasi Legislasi PerlindunganDataPribadi dalam Revolusi Industri 4.0," Jurnal Rechts Vinding, diterbitkan oleh Media PembinaanHukum Nasional, (Vol. 9 No. 2 Tahun 2020) : 244–245.

[6] Khudzaifah Dimyati dan Kelik Wardiono, Metode Penelitian Hukum, (Surakarta: UniversitasMuhammadiyah Surakarta, 2004), hlm. 7

[7] Soerjono Soekanto, dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, (Jakarta: Raja Grafindo Persada, 2010), hlm. 13-14.

Penulismempergunakan sifat penelitian deksriptif analitis, dalam proses pembahasan, data disajikan secara komprehensif, mendetail, dan terstruktur, dan kemudiandianalisis dengan mengacu pada kerangka teori dalamilmu hukumdanperaturan yang berlaku. Metode pendekatan pada penulisan hukumini.

Hasil dan Pembahasan

Tindak kejahatan cyberstalking seringkali menjadi langkah awal dalamterjadinya kejahatan dunia maya. Dalam tindakan cyberstalking, pelakuyangmelakukannya melakukan pengawasan terhadap target mereka denganmaksud mengumpulkan semua jenis informasi yang berkaitan data pribadi korban dengan memanfaatkan teknologi modern. Biasanya, pelaku memilihkorban karena iri hati atau perasaan dendam pribadi. Para pelaku cyberstalkingtidak menguntit korban secara langsung, tetapi mereka mengakses informasi milik korban melalui jejaring sosial media, yang digunakan untuk tujuan-tujuanyang tidak aman yang merugikan korban. Mereka menjalankan tindakanmereka melalui jaringan internet dengan menghimpun data seperti nama, alamat, riwayat keluarga, nomor telepon, kebiasaan harian, tanggal lahir, danelemen lainnya melalui jaringan media sosial. Setelah mendapatkandatapribadi ini, korban tindakan cyberstalking akan dilecehkan secara berulangolehpelaku, tindakan tersebut mencakup melakukan panggilan teleponyangmengandung pelecehan atau menyampaikan mengirimpesan ancamanterhadap seorang korban lewat jaringan internet. Bukan hanya itu, individuyangmelakukan tindakan tersebut dapat mengeksploitasi informasi ataupunberbagai data pribadi yang dimiliki korban dengan melakukan pengunggahankesitus web dengan isi yang mempunyai kaitan dengan konten seksual ataupunmenciptakan layanan kencan palsu dengan maksud menyerangataumemengaruhi emosi dan kesejahteraan mental orang lain.

Hukum yang mengatur cyberstalking dapat bervariasi dari satu yurisdiksi ke yurisdiksi lainnya. Beberapa yurisdiksi mungkin mensyaratkanadanya unsur-unsur tertentu, seperti penghinaan, pencemaran namabaik, pemerasan, ancaman, atau ancaman kekerasan yang terkandungdalamtindakan cyberstalking, agar tindakan cyberstalking dapat dikenakan sebagai tindakan ilegal. Ketentuan tersebut dapat berbeda-beda tergantungpadaperaturan di masing-masing wilayah hukum. Oleh karena itu, pentinguntukmemahami undang-undang yang berlaku di suatu wilayah dan elemen-elemenyang diperlukan untuk menentukan apakah suatu tindakan cyberstalkingdapat dianggap sebagai tindakan ilegal atau tidak dalam konteks hukumyangberlakudi sana.

Jika unsur-unsur seperti pencemaran nama baik, pelecehan, ancaman, pemerasan atau ancaman kekerasan terpenuhi, maka tindakan cyberstalkingtersebut dapat diadili sesuai dengan peraturan yang berlaku. Di Indonesia, peraturan yang menjadi dasar hukum dalam penanganan kejahatancyberstalking adalah Undang-Undang Republik Indonesia Nomor 19Tahun2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentangInformasi dan Transaksi Elektronik. Pasal-pasal yang relevan dalamUUITENomor 19 Tahun 2016 yang dapat dijadikan dasar hukumuntuk penuntutanterhadap cyberstalking adalah Pasal 27 ayat (3) dan ayat (4) jo. Pasal 45ayat (1). Pasal-pasal tersebut mengatur tindakan kriminal yang terjadi melalui teknologi dan jaringan internet serta memberikan dasar hukumuntukpenegakan hukum terhadap pelaku cyberstalking. Pasal-pasal tersebut mempunyai bunyi, yang berupat: Pasal 27 Ayat (3): “Setiap Orang dengan sengaja dan tanpahakmendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen

Elektronikyang memiliki muatan penghinaan dan/atau pencemaran nama baik". Pasal 27 Ayat (4): "Setiap Orang dengan sengaja dan tanpahakmendistribusikan 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 sebagaimanadimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ataudenda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".

Kaitan antara pelaku cyberstalking dengan Pasal 35 dalamUUITE, di mana manipulasi merujuk pada upaya oleh sekelompok orang atau individudalam melakukan penyerangan ataupun mempengaruhi emosi sertakesejahteraan mental seseorang dengan tujuan agar korban dapat dikendalikandan apa yang diinginkan oleh pelaku dapat diperoleh. Dalamkonteks tindakancyberstalking, manipulasi dapat mencakup berbagai taktik yang digunakanolehpelaku untuk merugikan dan mengganggu korban secara psikologis. Apabila pelaku cyberstalking dituntut di pengadilan dan dinyatakanbersalah, korban dapat mendapatkan keadilan melalui putusan pengadilan. Dalam proses hukum ini, pengadilan harus mempertimbangkan kerugianyangdialami korban, baik dalam bentuk kerugian materiil (seperti kerugian finansial) maupun kerugian immateriil (seperti kerugian psikologis dan emosional). Ini adalah langkah yang penting untuk memastikan bahwa korban cyberstalkingmendapatkan keadilan dan pemulihan setelah mengalami tindakan tersebut.

Permohonan ganti rugi yang diajukan sebagai respons terhadap putusanpengadilan adalah langkah hukum yang bersifat permanen dan mengharuskanpelaku untuk memberikan kompensasi kepada korban sebagai akibat dari kerugian yang dideritanya. Korban mendapat perlindungan oleh ketentuanganti rugi, yang memberikan hak kepada mereka untuk menerima kompensasi ataskerugian yang mereka alami sebagai hasil dari tindakan melawan hukumoranglain. Hal ini selaras dengan ketentuan Pasal 1365 KUHPerdata, yangmemberikan dasar hukum bagi kompensasi atas kerugian yang disebabkanoleh tindakan melawan hukum. Dengan demikian, korban memiliki hak untukmendapatkan ganti rugi sebagai bagian dari upaya untuk mengembalikan mereka ke kondisi sebelum tindakan melawan hukum tersebut terjadi.

Pengaturan lain yang dapat dijadikan dasar hukumuntuk kejahatancyberstalking adalah Pasal 310 ayat (1) dan (2) Kitab Undang-UndangHukumPidana (KUHP). Pasal 310 ayat 1 mengatur bahwa kehormatan atau nama baik seseorangdapat diserang dengan sengaja melalui tuduhan yang jelas ditujukanagar dikenal oleh masyarakat umum, dapat dikenai hukuman pencemaran denganancaman hukuman penjara maksimal sembilan bulan atau pencemaran dengandenda paling tinggi empat ribu lima ratus rupiah. Pasal 310 ayat 2 menjelaskanbahwa jika tindakan tersebut dilakukan dengan menggunakan tulisanataugambaran yang disebarkan, ditampilkan, atau ditempel di tempat umum, makapelakunya dapat dihukum dengan ancaman hukuman penjara selamasatutahun empat bulan atau denda paling tinggi empat ribu lima ratus rupiahkarenatindakan pencemaran yang dilakukan secara tertulis. Ketika kita merujuk pada kata "menyerang" dalam kutipan ayat pertama, dapat dilihat persamaan dengan tindakan cyberstalking yang seringkali melibatkan penyerangan dalam bentuk mencemarkan nama baik seseorang. Pelaku tindakan cyberstalking menggunakan kecanggihan teknologi untukmengumpulkan informasi pribadi tentang seseorang dan kemudianmenyebarkannya kepada masyarakat secara umum. Data yang didapatkantersebut seringkali dimanipulasi

menjadi berita yang merendahkanataumencemarkan kehormatan individu yang menjadi korban, yang mengakibatkankerugian bagi korban.

Dalam konteks hukum, jika seseorang terbukti melakukan tindakancyberstalking yang merusak reputasi seseorang melalui pesan teksataumengirim gambar yang merugikan, pelaku dapat menghadapi hukumanberdasarkan undang-undang yang berlaku. Sesuai dengan kutipan kedua, pelaku cyberstalking yang melibatkan pencemaran nama baik melalui teksatau gambaran mungkin akan dihukum dengan hukuman penjara yangtidakmelebihi satu tahun empat bulan atau denda sejumlah Rp 4.500. Hal ini bertujuan untuk memberikan sanksi yang sesuai dengan tingkat seriusnyatindakan cyberstalking dan memberikan perlindungan kepada korban. Membekali mereka dengan pemahaman tentang bagaimana melindungi data pribadi dan citra diri adalah langkah penting dalam memitigasi risiko ini.[8] Di Indonesia, sistem hukum belum secara tegas mengatur mengenai cyberstalking. Apabila merujuk kepada Undang-Undang yang berlaku saat ini, terdapat peraturan yang mendekati aspek-aspek dari cyberstalking yangbisadianggap sebagai perbuatan yang tidak diizinkan menurut Pasal 29 UUITEadalah tindakan yang melibatkan seseorang yang secara disengaja dantanpahak mengirimkan informasi elektronik dan/atau dokumen elektronik yangberisi ancaman kekerasan atau intimidasi yang ditujukan secara pribadi.

Pasal 29 UU ITE mengatur mengenai tindakan yang dapat merusakreputasi seseorang melalui media elektronik. Ancaman hukuman yangdapat dikenakan sesuai dengan Pasal 29 UU ITE adalah penjara dengandurasi maksimal selama 6 tahun dan/atau denda paling tinggi sebesar 1 miliar rupiah. Pasal 45 ayat (3) UU ITE menyangkut perbuatan menyebarkan informasi ataudokumen elektronik dengan maksud menciptakan rasa benci atau permusuhanterhadap individu atau kelompok tertentu. Hukuman yang mungkin dikenakanberdasarkan Pasal 45 ayat (3) adalah penjara dengan durasi hingga 6tahunpenuh dan/atau denda sebanyak 1 miliar rupiah pada tingkat maksimum. Jadi, kedua pasal ini mengatur sanksi yang serupa terkait dengan tindakanyangmelanggar hukum dalam domain digital. Karena hanya pemilik atau pihakyangmemiliki hak memiliki akses ke sistem elektronik. Selain itu, dalamsatusistemelektronik, terdapat nilai-nilai, termasuk nilai-nilai pribadi dan ekonomis, sehingga ketentuan dalam pasal ini bertujuan melindungi privasi dankepentingan pemilik atau pihak yang berhak tersebut. Kolaborasi antara berbagai pihak, termasuk pemerintah, lembaga hukum, pendidik, dan masyarakat sipil, menjadi kunci dalam menciptakan lingkungan informasi yang lebih sehat dan bermartabat di era digital ini.[9]

Kesimpulan

Dengan pesatnya perkembangan teknologi, kejahatan yang berasal dari kemajuan teknologi, termasuk cyberstalking, semakin meningkat. Olehkarenaitu, diperlukan regulasi yang spesifik untuk mengelola aksi cyberstalking. Padamenyelesaikan isu regulasi yang berkaitan dengan kejahatan cyberstalking, perlu ada undang-undang pidana yang menjelaskan

[8] Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis Hukum terhadap Upaya Pencegahan Kasus Deepfake Porn dan Pendidikan Kesadaran Publik di Lingkungan Digital. *Jurnal Pendidikan Tambusai*, *7*(3), 26179–26188.

[9] Utama, A. N., Hidayat, R. M., Kesuma, P. T., & Hosnah, A. U. (2023). Analisis Hukum Pencegahan Hoax terhadap Fatwa MUI Terkait Boikot Produk dan Pendidikan Kesadaran Publik dalam Era Digital. Jurnal Pendidikan Tambusai, 7(3), 30323–30334.

seseorang yangsecarasengaja menjalankan pengejaran kepada seseorang yang dilaksanakan melalui internet, dengan mengirimkannya sebuah ataupun beberapa pesan elektronikdengan kesadaran terhadap orang lain juga aksinya tersebut mengganggu seseorang, akan dihadapkan pada ancaman hukuman.

Namun, penting untuk mengklasifikasikan tindakan cyberstalkingsebagai kejahatan yang dapat diadukan dengan batasan yang jelas, danpadapenerapan sanksi, seluruh lembaga hukum perlu mempertimbangkan keadaanmental pelakunya. Selain itu, perlindungan data pribadi semakin pentingdi eradigital ini. Sebagai respons terhadap perkembangan teknologi dan potensi risiko cyberstalking, peraturan perlindungan data pribadi juga harus diperkuat untuk memastikan bahwa individu memiliki hak dan privasi yang dijaga secaraketat dalam dunia maya. Ini akan membantu melindungi individu dari berbagai tindakan cyberstalking dan penyalahgunaan data pribadi.

Saran

Kami menyarankan untuk perlu dilakukan langkah-langkah untuk menciptakan undang-undang pidana yang secara khusus mengatasi masalah cyberstalking. Ini harus mencakup definisi yang jelas dan kriteria tindakan cyberstalking. Kemudian penting untuk menetapkan sanksi yang seimbang dan tegas bagi pelaku cyberstalking, termasuk denda yang signifikan dan ancaman hukuman penjara untuk memberikan efek pencegahan. Diperlukan sistem pengelompokan yang membedakan tindakan cyberstalking dari perilaku online lainnya agar penerapan undang-undang dapat lebih efisien. Saat menetapkan sanksi, harus mempertimbangkan kesehatan mental pelaku untuk memilih sanksi yang sesuai dengan kondisinya.

Regulasi perlindungan data pribadi perlu diperkuat untuk mengatur dengan lebih ketat pengelolaan data pribadi dan mengurangi risiko penyalahgunaan dalam konteks cyberstalking. Kampanye pemberitahuan perlu ditingkatkan untuk meningkatkan kesadaran masyarakat tentang risiko cyberstalking dan cara melindungi diri online. Kemudian dengan mendorong kolaborasi antara lembaga hukum, keamanan siber, dan penyedia layanan internet di tingkat global untuk menghadapi cyberstalking secara efektif. Lalu perlu dibangun sistem dukungan untuk membantu korban cyberstalking dalam melaporkan insiden, melindungi data pribadi, dan mendapatkan bantuan hukum yang dibutuhkan.

Daftar Pustaka

Adiningsih, Sri. Transformasi Ekonomi Berbasis Digital di Indonesia, Jakarta: GramediaPustaka Utama, 2019.

Dimyati, Khudzaifah dan Kelik Wardiono. Metode Penelitian Hukum. Surakarta: Universitas Muhammadiyah Surakarta, 2004.

Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis Hukum terhadap Upaya Pencegahan Kasus Deepfake Porn dan Pendidikan Kesadaran Publik di Lingkungan Digital. *Jurnal Pendidikan Tambusai*, *7*(3), 26179–26188. Retrieved from https://jptam.org/index.php/jptam/article/view/10815

Halaman Utama Dema Justicia Fakultas Hukum Universitas Gadjah Mada. DemaJusticia, diterbitkan oleh: Fakultas Hukum Universitas Gadjah Mada, tersedia di: https://demajusticia.org/, diakses 3 November 2023.

Pittaro, Michael L. "Cyberstalking: An Analysis of Online Harassment and Intimidation". International Journal of Cyber Criminology. Vol. 1 No. 2 Tahun 2007.

Sinaga, Erlina Maria Christin dan Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0". Jurnal RechtsVinding, diterbitkan oleh Media Pembinaan Hukum Nasional. Vol. 9No. 2Tahun 2020.

Soekanto, Soerjono, dan Sri Mamudji. Penelitian Hukum Normatif Suatu TinjauanSingkat. Jakarta: Raja Grafindo Persada, 2010.

Sunarso, Siswanto. Hukum Informasi dan Transaksi Elektronik. Jakarta: Rineka Cipta, 2009.

Utama, A. N., Hidayat, R. M., Kesuma, P. T., & Hosnah, A. U. (2023). Analisis Hukum Pencegahan Hoax terhadap Fatwa MUI Terkait Boikot Produk dan Pendidikan Kesadaran Publik dalam Era Digital. Jurnal Pendidikan Tambusai, 7(3), 30323–30334. Retrieved from https://jptam.org/index.php/jptam/article/view/11901