Jurnal Hukum, Politik dan Ilmu Sosial
Vol.3, No.4 Desember 2024
e-ISSN: 2963-7651; p-ISSN: 2963-8704, Hal 232-241
DOI: https://doi.org/10.55606/jhpis.v3i4.4454
Available Online at: https://ejurnal.politeknikpratama.ac.id/index.php/jhpis

Tinjauan Yuridis Terhadap Ancaman dan Upaya Penanggulangan Tindak Pidana Perundungan di Dunia Maya (*Cyberbullying*)

Kayla Astrida Aristianto
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Bandar Lampung, Indonesia
Korespondensi Penulis : *kayla17092002@gmail.com*

Abstract. *Current technological advances have positive and negative effects. While there are many benefits to be gained from this advancement, it also has many negative effects for users. The number of crimes that occur in cyberspace, such as cyberbullying, is one of the negative impacts that must be addressed and must be followed up when imposing sanctions on perpetrators. Because it has had a negative impact on victims of cyberbullying, the perpetrator must be given a deterrent punishment. Normative juridical research methods were used in this research, and the data collection method used was literature study. The government has established laws regarding the criminal act of cyberbullying, as stated in the Criminal Code and the ITE Law. The aim of this law is to eradicate and minimize cyberbullying perpetrators and acts.*

Keyword: *Cyberbullying, crimes, sanction*

Abstrak. Kemajuan teknologi saat ini memiliki efek positif dan negatif. Meskipun ada banyak manfaat yang dapat diperoleh dari kemajuan ini, kemajuan ini juga memiliki banyak efek negatif bagi pengguna. Jumlah kejahatan yang terjadi di dunia maya, seperti cyberbullying, merupakan salah satu dampak negatif yang harus ditanggulangi dan harus ditindak lanjuti saat memberikan sanksi kepada pelaku. Karena telah berdampak buruk pada korban cyberbullying, pelaku harus dikenakan hukuman jera. Metode penelitian yuridis normatif digunakan dalam penelitian ini, dan metode pengumpulan data yang digunakan adalah studi kepustakaan. Pemerintah telah menetapkan undang-undang tentang tindak pidana cyberbullying, seperti yang tercantum dalam KUHP dan UU ITE. Tujuan dari undang-undang ini adalah untuk memberantas dan meminimalkan pelaku dan tindakan cyberbullying.

Kata Kunci: *Cyberbullying*, kejahatan, sanksi

1. LATAR BELAKANG

Berkembangnya zaman saat ini juga berpengaruh pada pesatnya kemajuan teknologi dan memberikan pengaruh perubahan sosial salah satunya fenomena kejahatan.Fenomena kejahatan merupakan permasalahan yang terus melekat dalam masyrakat, baik pada tiap-tiap individu. Tidak hanya pada kehidupan nyata sehari-hari saja, fenomena kejahatan juga banyak kita jumpai pada dunia maya atau *cyberspace.*

Cyberspace atau dunia maya merupakan ruang digital yang terkoneksi padajaringan internet yang tersebar luas, bahkan keseluruh dunia untuk media komunikasi online. Namun, *cyberspace* saat ini banyak disalahgunakan dan keluar dari fungsi *cyberspace* sebenarnya. Banyak kejahatan yang dilakukan oleh oknum individu atau kelompok di dunia maya, yang biasa disebut sebagai *cybercrime.*

Received September 14, 2024; Revised Oktober 05, 2024; Accepted Oktober 30, 2024; Online Available November 05, 2024

Cybercrime adalah fenomena kejahatan yang terjadi di dunia maya, yang memberikan dampak negatif seperti munculnya hacker, pembajakan, bahkan peundungan yang memiliki tujuan untuk memperoleh keuntungan materil maupun non materil bagi pelaku *cybercrime,* seperti menghasilkan uang, ancaman pemerasan, memberikan gangguan kepada seseorang, mempermalukan seseorang, meretas informasi atau data pribadi seseorang atau kelompok.

Salah satu jenis fenomena kejahatan dunia maya yang sering terjadi adalah *cyberbullying. Cyberbullying* adalah suatu tindakan intimidasi, pengucilan, merendahkanatau memberi ancaman pihak lain pada ruang digital. *Cyberbullyin*g bisa terjadi diberbagai kalangan, baik orang dewasa, remaja atau anak-anak dibawah umur dan bisa terjadi kapan saja dan dimana saja pada siapapun.

Dengan ini, pemerintah memberikan regulasi untuk menangani serta meminimalisir tidakan *cyberbullying*. Yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik perubahan atas Undang-UndangNomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dilihat dari latar belakang yang telah dipaparkan, dapat ditarik bahwa rumusan masalah penelitian ini adalah Bagaimana penerapan sanksi terhadap pelaku *cyberbullying*? Dan bagaimana upaya penanggulangan serta pencegahan *cyberbullying* saat ini?.

2. METODE PENELITIAN

Metode yuridis normatif dengan pendekatan peraturan perundang-undangan adalah metode yang digunakan dalam penelitian ini. Data sekunder yang digunakan dalam penelitian ini berasal dari bahan hukum primer, sekunder, dan tersier. Metode pengumpulan data yang digunakan adalah studi kepustakaan, dengan data dan informasi yang diperoleh berasal dari berbagai jenis sumber, seperti buku, dokumen, artikel, dll. Penelitian ini bertujuan untuk mengidentifikasi jenis ancaman yang terkait dengan sanksi yang diberikan kepada pelaku tindak pidana cyberbullying serta upaya apa saja yang perlu dilakukan untuk menangani atau mencegah tindakan cyberbullying kembali terjadi pada masyarakat.

3. PEMBAHASAN

Tinjauan Ancaman Pidana Pelaku *cyberbullying*

Cybercrime memiliki ciri unik dibandingkan dengan kejahatan konvensional lainnya, sehingga dikategorikan sebagai kejahatan baru. Cybercrime muncul seiring dengan perkembangan teknologi informasi. "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi," kata R. Nitibaskara. Kejahatan, penyimpangan hubungan sosial, akan menyesuaikan diri dengan karakter baru ini melalui interaksi seperti ini..

Salah satu fenomena kejahatan siber yang marak terjadi saat ini ialah *cyberbullying.* Tindakan intimidasi atau perundungan terhadap seseorang yang dapat memberikan dampak pada psikologis seperti stress, depresi, hingga rasa keterpurukan bagi korban. *Cyberbullying* terdiri dari beberapa aspek, yaitu:

1) *Flaming,* yaitu perdebatan secara langsung melalui media online dengan mengirimkan teks bahasa yang kasar atau menyebar foto yang bersifat menghina.
2) *Harrasement,* yaitu tindakan berupa komunikasi digital melalui berbagai macam media yang menyinggungsecara berulang dalam dalam kurun waktu yang lama.
3) *Denigration,* yaitu menyebarkan secara online informasi pribadi milik seseorang untuk merusak reputasi hingga menimbulkan ketidaknyamanan.
4) *Impersonation,* yaitu berpura-pura menjadi orang lain dan/atau bertindak atas nama seseorang dan menyampaikan beberapa pesan yang menyinggung orang lain.
5) *Putting and Trickery,* yaitu menyebarkan foto atau informasi tanpa izin yang dimana sifatnya sensitif atau privasi milik seseorang atau penipuan terhadap seseorang agar memberikan foto pribadinya.
6) *Excluxion,* yaitu dengan sengaja mengeluarkan seseorang dari suatu komunitas untukmengisolasinya.
7) *Cyberstalking,* yaitu melakukan ancaman atau intimidasi yang sering berkelanjutanmelalui internet.

Tindakan *cyberbullying* ini marak terjadi di Indonesia. Salah satu tindakan *cyberbullying* adalah *body shaming* oleh netizen, akibat dari hal tersebut dapat membuat korban kehilangan kepercyaan dirinya. Hal ini merupakan bukti nyata

dari dampak negatif dari *cyberbullying*. Pemerintah perlu memberikan sanksi yang tegas kepada para pelaku *cyberbullying* di Indonesia. Dalam menanggapi kasus *cyberbullying* yang terjadi di Indonesia, pemerintah mengeluarkan Uundang-Undang (UU) yang mampu memberikan kepastian hukum kepada para pelaku *cyberbullying* di Indonesia. Undang- Undang tentang *cyberbullying* diatur dalam KUHP dan UU ITE.

Tinjauan ancaman bagi pelaku tindak pidana *cyberbullying* termuat dalam Undang- Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pada pasal 27 ayat (3) Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa "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 28 ayat (2) Undang-Undang Informasi dan Trasaksi Elektronik disebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA)".

Diatur juga sanksi pidana bagi pelaku *cyberbullying* sebagaimana yang telah disebutkan pada pasal 27 ayat (3) dan pasal 28 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Sanksi pidana tersebut diatur dalam pasal 45 ayat (1) bahwa "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)". Pasal 45 ayat (2) menyatakan ancaman pidana sebagaimana yang disebutkan pada pasal 28 ayat (2), yaitu: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Upaya Penanggulangan Serta Pencegahan *Cyberbullying*

Terdapat beberapa aspek penting yang perlu dipertimbangkan secara mendalam dalam menanggulangi *cyberbullying*.

1. Kemajuan teknologi saat membuka berbagai kejahatan siber (*cybercrime)*. Dengan berbagai cara serta upaya untuk melakukan *cybercrime,* oleh karena itu Cyber Law harus diperbaharui seiring berkembangnya teknologi saat ini. Dengan tujuan untuk memperkuat penegakkan hukum dalam ruang digital serta memberikan kepastian hukum dan menjamin keadilan terhadap korban *cybercrime*.
2. Kolaborasi antara pemerintah sangat dibutuhkan, baik dengan lembaga penegak hukum, sektor swasta, dan masyarakat sipil dalam menangani *cybercrime*. Kerjasama lintas sektoral dan internasional diperlukan untuk memastikan pertukaran informasi yang efektif, pengembangan teknologi keamanan yang canggih, dan penegakanhukum yang konsisten terhadap pelaku kejahatan siber. Sistematisasi inilah yang menjadilandasan bagi upaya penanggulangan *cybercrime*.
3. Pelaksanaan *Cyberlaw* harus dengan aparat penegak hukum yang tegas namun, masih dengan menjaga penghormatan hak asasi manusia. Sangat penting dalam menegakkan hukum serta pemberian sanksi kepada pelaku kejahatan siber, tetapi dalam penegakkannya harus dipastikan bahwa tidak melanggar hak-hak individu, seperti kebebasan berekspresi dan privasi.
4. Edukasi dan kampanye kesadaran publik adalah kunci dalammemberikan pemahaman serta merubah pola pikir masyarakat terhadap keamanan digital.Melalui upaya tersebut, masyarakat jadi mengetahui dengan baik mengenai risiko *cybercrime* serta langkah-langkah yang dapat harus dilakukan untuk melindungi diri, individu dan organisasi dapat menjadi lebih proaktif dalam melawan *cybercrime*.
5. Penelitian berkelanjutan adalah salah satu upaya guna menghadapi ancaman yang begitu pesat pada *cyberspace* seperti, pengembangan sistem deteksi, kecerdasan dalam menganalisis data, serta keamanan jaringan yang canggih.

6. Penegakan hukum terhadap pelaku kejahatan siber harus dilakukan dengan sangat tegas, efektif, serta. Yang mencakup penyelidikan yang cermat, pengumpulan bukti digital yang sah, serta penggunaan metode penegakan hukum yang sesuai dengan sistem keadilan di Indonesia. Selain itu, penting juga untuk meningkatkan kapasitas penegak hukum dalam *cybercrime* yang berkualitas melalui pelatihan dan kerjasama lintas sektoral.
7. Pembaharuan hukum siber harus mempertimbangkan perkembangan teknologi serta masalah yang terus dihadapi dalam kejahatan siber. Kebijakan yang dapat menyesuaikan diri dengan kemajuan teknologi seperti saat ini membuat sistem penegakan hukum di dunia digital lebih efisien dan relevan.
8. Indonesia harus aktif terlibat dalam forum regional dan internasional serta bekerja sama dengan negara lain dalam upaya penanggulangan cybercrime untuk saling berbagi informasi, berbagi sumber daya, dan mengkoordinasi tindakan dengan negara lain untuk menghadapi ancaman cybercrime lintas negara. Sangat penting untuk melakukan evaluasi berkala terhadap efektivitas undang-undang internet dan metode pencegahan cybercrime. Evaluasi teratur dapat membantu menemukan masalah dan kekurangan penegakan di dunia digital dan melakukan perbaikan.
9. Transparansi dan akuntabilitas adalah elemen penting dalam penanganan kejahatan siber. Pemerintah dan lembaga penegak hukum perlu melakukan komunikasi yang terbuka dengan masyarakat tentang upaya-upaya penanggulangan *cybercrime*, termasuk kasus-kasus yang terungkap dan implementasi hukum yang dilakukan bagi pelaku *cybercrime*. Dengan ini masyarakat bisa lebih percaya diri dalam melaporkan serta mendukung upaya penanggulangan *cybercrime*.
10. Integrasi antara sektor publik dan swasta dapat memperkuat strategi penanggulangan cybercrime. Pemerintah dan lembaga penegak hukum perlu berkomunikasi dengan masyarakat tentang upaya penanggulangan cybercrime, termasuk kasus-kasus yang terungkap dan tindakan hukum yang diambil terhadap pelaku cybercrime. Banyak perusahaan swasta memiliki sumber daya dan keterampilan yang sangat berharga dalam bidang keamanan informasi yang dapat digunakan untuk memerangi tindakan kriminal cyber. Sangat penting bagi sektor swasta untuk bekerja sama dengan pemerintah

dalam hal pertukaran informasi, sumber daya, dan pelatihan. Seperti itu, keamanan siber publik-swasta dapat membantu orang bekerja sama dengan baik untuk memerangi cybercrime.

11. Pentingnya pendidikan dan pelatihan dalam membangun kapasitas masyarakat guna menghadapi *cybercrime* jangan sampai terabaikan. Program-program pendidikan yang ditujukan untuk berbagai kalangan serta kelompok, mulai dari pelajar hingga profesional, perlu dikembangkan untuk meningkatkan pemahaman mengenai risiko *cybercrime* dan keterampilan untuk melindungi diri secara efektif. Dengan peningkatan pengetahuan serta pemahaman digital dan keamanan informasi, masyarakat dapat menjadi lebih tangguh dan responsif terhadap ancaman kejahatan siber yang terus berkembangan.

Dalam kaitan dengan upaya pencegahan tindak pidana, UU ITE menjadi dasar hukum dalam proses penegakan hukum kejahatan-kejahatan siber atau ruang digital, termasuk kejahatan pencucian uang dan kejahatan terorisme (Saefullah. 2009).

Penegakkan hukum *cybercrime* sebelum disahkannya UU ITE dilakukan dengan menafsirkan *cybercrime* ke dalam perundang- undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi diantaranya: (Zainudin Hasan. 2024)

1. Undang – Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik;
2. Undang -Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
3. Undang-Undang No. 19 tahun 2002 sebagaimana telah diubah oleh UndangUndang No. 28 Tahun 2014 tentang Hak Cipta;
4. Undang-Undang No. 25 Tahun 2003 tentang Perubahan atas Undang – Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang sebagaimana telah diganti dengan Undang-Undang No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
5. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme; Dan lain sebagainya.

Dalam perkembangannya, pengaturan *cyberspace* dan kejahatan siber

diatur di dalam Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi DanTransaksi Elektronik sebagai payung hukum. UU ITE diharapkan sebagai pengendali danpenegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.

Dalam hal ini, peningkatan kesadaran masyarakat tentang risiko dan ancaman cybercrime yang berkembang pesat sangatlah penting. Tidak hanya masyarakat yang harus sadar hukum, tetapi aparat penegak hukum juga harus sadar hukum. Tanpa kesadaran ini, sistem penegakan keadilan, pemanfaatan, dan pencegahan ancaman dunia digital akan gagal. Menurut Ikdik M. Arief Mansur dan Elisatris Gultom, ada beberapa alasan mengapa kesadaran hukum masyarakat Indonesia masih rendah hingga saat ini. Salah satunya adalah kurangnya pemahaman dan pengetahuan tentang jenis kejahatan di ruang digital atau cybercrime.

Kekurangan pengetahuan ini menghambat upaya penanggulangan cybercrime, yang menyebabkan hambatan dalam penaatan hukum dan proses pengawasan masyarakat pada setiap aktivis yang terlibat dalam cybercrime. Dengan demikian, tepat dikatakan jika penegakan hukum yang optimal memerlukan kesadaran hukum dan kesadaran moral dari masyarakat maupun dari aparat atau lembaga penegak hukum itu sendiri.

4. KESIMPULAN DAN SERUM

Kesimpulan

Tindak kejahatan pada ruang digital (*cyberspace)* seperti *cyberbulying* yang kian pesat harus diberikan sanksi yang memiliki efek jera bagi sang pelaku, karena dampak yang dirasakan oleh korban seperti, stress, depresi, dan lainnya yang sifatnya berkelanjutan. Saat ini, sudah ada peraturan yang membahas tindak pidana untuk pelaku *cyberbullying* yang termuat dalam KUHP dan UU ITE dengan ancaman pidana bagi pelaku tindak pidana *cyberbullying* termuat dalam pasal 27 ayat (3), pasal 28 ayat (2), serta pasal 45 ayat (1) Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Kasus *cyberbullying* yang terjadi di Indonesia merupakan hal yang cukup serius dan

harus ditangani secara tepat karena telah merugikan banyak pihak. Keefektikan dalam pemberantasan cyberbullying harus diikuti oleh kesadaran masyarakat itu sendiri serta ketegasan dari aparat hukum dalam menindaklanjuti kasus *cyberbullying*.

Saran

Berdasarkan uraian diatas, berikut adalah beberapa saran yang dapat dipertimbangkan:

1. Penegasan pada regulasi yang mengatur tindak pidana *cyberbullying* perlu dilakukan oleh pemerintah agar muncul rasa takut pada diri pelaku *cyberbullying* dan meminimalisir terjadinya kasus *cyberbullying* di Indonesia.
2. Peran sekolah serta lembaga pendidikan lainnya pun sangatlah penting dalam mendidik generasi bangsa, guna membentuk individu yang baik dan memiliki rasa empati, simpati, kasih sayang, serta menjaga satu sama lain, bukan justru menindas individu lainnya.
3. Kebijaksanaan dalam menggunakan media sosial juga seharusnya sudah menjadi sebuah hal yang melekat pada penggunanya dengan ini, kejahatan pada dunia digital atau *cybercrime* perlahan akan berkurang atau bahkan diharapkan tidak ada lagi kejahatan siber yang menimbulkan korban.
4. Kesadaran dari tiap-tiap individu serta peran keluarga dalam upaya menanamkan pemahaman mengenai dampak atau keburukan dalam dunia digital dan berbagai hal positif yang seharusnya dapat ditemukan pada dunia digital yang semakin modern.

DAFTAR PUSTAKA

Dewi, N. N. A. P., Nahak, S., & Widyantara, I. M. M. (2021). Pembuktian tindak pidana intimidasi melalui media sosial (cyberbullying). Jurnal Analogi Hukum, 3(1), 90–95.

Hasan, Z., & Weliyansyah, G. (2024). Analisis hukum pidana terhadap tindak pidana perundungan di ruang maya (cyberbullying): Perspektif hukum pidana di Indonesia. Jurnal Hukum dan Kewarganegaraan, 5(4).

Hasan, Z., Alfath, M. R., Mahardika, A., Rizaldi, R., & Rizqullah H. W. (2024). Peranan cyber law dalam penanganan tindak pidana di Indonesia. Jurnal Komunikasi, 2(5), 337–345.

Hasan, Z., Yansah, A., Wijaya, B. S., Salsabila, R. F., Sarenc, S. B., & Salim, A. A. P.

(2024). Tinjauan cyberlaw terhadap ancaman dan strategi penanggulangan cybercrime. MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora, 2(2), Juni.

Koops, B. J. (2017). The Routledge handbook of technology, crime, and justice. Routledge.

Riquelme, F., & Prato, C. (2017). The dark side of the web: Assessing web crime and cyber deviance. International Journal of Cyber Criminology.

Sahat Maruli T. Situmeang, S. H., M. H. (2020). Cyber law. Bandung.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.

Spinello, R. A., & Tavani, H. T. (2016). Cyberethics: Morality and law in cyberspace (5th ed.). Jones & Bartlett Learning.

Sumantri, S., et al. (2022). Edukasi pentingnya mengantisipasi cyberbullying yang marak terjadi di media sosial. National Conference for Community Service Project (NaCosPro), 4(1), 424–428.