Lex LATA
Jurnal Ilmiah Ilmu Hukum

Kantor Editor: Program Studi Magister Ilmu Hukum Fakultas Hukum Palembang
Sumatera Selatan-30139 Indonesia.
Telepon: +62711-580063 Fax: +62711-581179
E-mail : lexlata@fh.unsri.ac.id
Website : http://journal.fh.unsri.ac.id/index.php/LexS

ISSN Print:
e-ISSN: 2657-0343

PENGATURAN DAN PENEGAKAN HUKUM KEJAHATAN DUNIA MAYA (CYEBER CRIME) : HARMONISASI REVISI UNDANG-UNDANG ITE DAN KUHP

Martini Idris, Serlika Aprita*, Meirina Nurlani

Abstrak : *Cyber crime* merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi melalui internet. Fenomena *cyber crime* di Indonesia merupakan perbincangan yang selalu menarik minat masyarakat. Dari masyarakat pada umumnya, sampai pada masyarakat yang memang memiliki keterkaitan langsung dengan fenomena *cyber crime.* Misalnya, aparat penegak hukum, akademisi khususnya akademisi hukum. Metode penelitian yang digunakan dalam penelitian ini adalah hukum normatif yang berfokus pada kajian berdasarkan pada doktrin yang berdasarkan atas peraturan perundang-undangan maupun putusan pengadilan yang bersifat primer, sekunder, dan tersier. Hasil penelitian yang dapat dijadikan sebagai kesimpulan dalam penelitian ini terdapat beberapa kekurangan dalam upaya penegakan hukumnya, sanksi yang dikenakan masih ringan. Padahal beberapa kasus mengakibatkan kerugian yang besar sehingga tidak sesuai dengan akibat yang ditimbulkan. Kendala dalam penegakan hukum terhadap *cyber crime* antara lain karena kurangnya fasilitas dan sarana, minimnya kemampuan penegak hukum, dan tidak ada unit khusus yang menangani kasus *cyber crime.* Sehubungan dengan itu, rancangan konsep KUHP yang baru telah dilaksanakan untuk melihat kebijakan hukum ke depan dalam memberantas dan menegakkan hukum yang berkaitan dengan kejahatan dunia maya dan revisi UU ITE diperlukan untuk mengoptimalkan penegakan hukum terhadap *cyber crime* di Indonesia.

Kata Kunci: Hukum Pidana ; Kejahatan ; C*yber Crime*

Abstract : *Cyber crime is a crime committed using information technology, namely by using the internet. The phenomenon of cyber crime in Indonesia is a topic of discussion that always attracts public interest. From society in general, to people who are directly related to the phenomenon of cyber crime. For example, law enforcement officers, academics, especially legal academics. The research method used in this research is normative law because the focus of the study is based on doctrine through analysis of legal rules found in statutory regulations or in various court decisions using primary, secondary and tertiary research materials. The research results that can be used as conclusions in this research still contain several shortcomings in law enforcement efforts, in fact the sanctions imposed when using the Criminal Code are indeed light. In fact, some cases that occur*

result in large losses that are not commensurate with the consequences. Obstacles in law enforcement against cyber crime include, among other things, a lack of facilities and means, a lack of law enforcement capacity, and the absence of a special unit that handles cyber crime cases. In this regard, a draft concept of the new Criminal Code has been implemented to look at future legal policies in eradicating and enforcing laws relating to cyber crime and revision of the ITE Law is needed to optimize law enforcement against cyber crime in Indonesia.

Keywords: *Criminal Law ; Crime ; Cyber Crime*

Riwayat Artikel:
Diterima : 15 Maret 2024
Revisi : 21 Oktober 2024
Disetujui : 27 Oktober 2024

DOI: 10.28946/lexl.v6i3.4266
*Fakultas Hukum Universitas Muhammadiyah Palembang, Fakultas Hukum Universitas Muhammadiyah Palembang, Fakultas Hukum Universitas Sjakhyakirti.
Email: 5312lika@gmail.com , meirina_nurlani@unisti.ac.id

LATAR BELAKANG

Globalisasi dan segala perkembangannya menawarkan janji-janji yang sangat menarik manusia. Hal ini dikarenakan globalisasi yang melahirkan ilmu pengetahuan dan teknologi yang amat membantu manusia. Ilmu pengetahuan dan teknologi telah menghasilkan sarana prasarana, piranti-piranti dan alat-alat yang mempermudah manusia dalam berbagai aktifitasnya. Pada intinya ilmu pengetahuan dan teknologi memberikan sesuatu yang memiliki nilai guna kepada manusia. Perkembangan globalisasi dan era teknologi saat ini membuat segala sesuatunya yang dahulu amat sulit dilakukan menjadi mudah dan serba otomatis. Globalisasi dalam bidang teknologi telekomunikasi telah mempersempit wilayah dunia dan memperpendek jarak komunikasi. Sebagai contoh bahwa media elektronika komputer dengan jejaring internet membuat komunikasi menjadi tanpa batas dan dapat dilakukan oleh siapapun dan dimanapun. Arus globalisasi saat ini sedang menuju era serba digital (*digital world)* dengan kemajuan teknologi informasi dan komunikasi. Oleh karena itu, sangat menggembirakan melihat kemajuan dunia yang rumit, beragam, dan pluralistik, karena pertumbuhan teknologi komputer dan internet telah menjadi instrumen baru bagi negara-negara di dunia untuk digunakan sebagai alat penetrasi, pengaruh, dan infiltrasi ke

berbagai negara.[1] Sebagai hasil dari globalisasi, negara-negara dapat berdagang secara bebas satu sama lain, melewati kekuatan hegemonik dalam prosesnya.Perang ekonomi, sosial, dan budaya pecah sebagai hasil dari upaya masing-masing bangsa untuk tumbuh secara ekonomi, sosial, dan budaya. Konflik energi, konflik pangan, dan konflik air semuanya meningkat sebagai akibat dari negara-negara yang bersaing untuk menguasai sumber daya yang langka atas nama globalisasi, perdagangan bebas, dan pasar bebas. Baik di masa kini maupun masa depan, teknologi informasi akan menjadi sangat penting. Negara-negara di seluruh dunia berharap dapat menuai beberapa keuntungan dan peluang berkat kemajuan teknologi informasi. Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J.E Sahetapy menyatakan bahwa kejahatan erat kaitannya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.[2]

Berbicara mengenai kejahatan, maka secara empiris definisi kejahatan dapat dilihat dari dua perspektif, *pertama* adalah kejahatan dalam perspektif yuridis, kejahatan yang dirumuskan sebagai perbuatan yang oleh negara diberi pidana. Pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang tertanggu akibat perbuatan itu. Perbuatan atau kejahatan yang dalam ilmu hukum pidana biasa disebut dengan tindak pidana (*strafbaarfeit*). *Kedua*, kejahatan dalam arti sosiologis (kriminologis) merupakan suatu perbuatan yang dari sisi sosiologis merupakan kejahatan sedangkan dari segi yuridis (hukum positif) bukan merupakansuatu kejahatan. Artinya, perbuatan tersebut oleh negara tidak dijatuhi pidana. Kejahatan adalah suatu tindakan anti sosial yang merugikan, tidak pantas, tidak dapat dibiarkan, yang dapat menimbulkan kegoncangan dalam masyarakat. Sedangkan Van Bemmelen merumuskan, kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, dan menimbulkan begitu banyak ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat

[1] Widodo Dwi Putro, "Pancasila Di Era Paska Ideologi," *Jurnal Veritas et Justitia* 5, no. 1 (2019): 1–19.
[2] Insan Pribadi, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," *Jurnal Lex Renaissance* 3, no. 1 (2018): 109–24.

itu berhak mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapadengan sengaja diberikan karena kelakuan tersebut. Dari pengertian tersebut dapatdisimpulkan bahwa unsur penting dari pengertian kejahatan adalah, perbuatan yanganti sosial, merugikan dan menimbulkan ketidaktenangan masyarakat serta bertentangan dengan moral masyarakat. Namun hal tersebut dapat mengalamipergeseran cara pandang yang dipengaruhi oleh faktor moral masyarakat karena moral masyarakat menjadi tolok ukur perbuatan itu jahat atau tidak.

Salah satu bentuk kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitandengan aplikasi internet. Kejahatan ini dalam istilah asing disebut *Cybercrime*. Barda Nawawi Arief menggunakan istilah tindak pidana mayantara untuk menunjuk jenis kejahatan ini atau idsentik dengan "tindak pidana siber" (*cyberspace*).[3] Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua bagian besar. Pertama, kejahatan yang bertujuan merusakatau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer dan internet sebagai alat bantu dalam melancarkan kejahatan. Namun, mengingat teknologi informasi (telekomunikasi, komputer dan media) dapat berkembang seiring waktu maka kejahatan jenis diatas dapat berkembang menjadi lebih luas lagi.

METODE PENELITIAN

Metode ilmiah dari suatu ilmu pengetahuan yaitu segala cara dalam rangka ilmu tersebut, untuk sampai kepada kesatuan pengetahuan. Tanpa metode ilmiah, suatu ilmu pengetahuan itu sebenarnya bukan suatu ilmu, tetapi suatu himpunan pengetahuan saja tentang berbagai gejala, tanpa dapat disadari hubungan antara gejala yang satu dengan gejala lainnya.[4] Penelitian yang akan digunakan adalah penelitian hukum dalam tataran teori yang diperlukan untuk mengembangkan suatu bidang kajian hukum tertentu. Hal ini dilakukan untuk meningkatkan dan memperkaya pengetahuan dalam penerapan aturan hukum. Dengan melakukan telaah mengenai sanksi pidana dan juga mampu menggali teori-teori yang ada di belakang ketentuan hukum tersebut.[5] Metode penelitian yang digunakan oleh penulis adalah metode penelitian hukum normatif, artinya penelitian yang di fokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif.[6]

---

[3] S Januar Ashady, "Cybercrime Sebagai Kejahatan Dunia Maya Dalam Perspektif Hukum Dan Masyarakat," *Jurnal Jurisdische* 1, no. 2 (2024): 34–46.
[4] Muslimah, "Kajian Filsafat Ilmu Dalam Kebudayaan," *Bangun Kaprima : Jurnal Pengembangan Rekayasa Sosial Dan Humaniora* 07, no. 2 (2021): 108.
[5] Peter Mahmud Marzuki, "Penelitian Hukum," Revisi (Jakarta: Prenada Media, 2017).
[6] Johnny Ibrahim. 2005. *Teori Dan Metode Penelitian Hukum Normatif*. Jakarta: Bayumedia Publishing

Penelitian hukum normatif adalah penelitian hukum yang menggunakan data sekunder atau sumber data yang berasal dari bahan kepustakaan (*library research*), yakni penelitian yang dilakukan dengan cara melakukan penelitian terhadap berbagai sumber bacaan seperti buku-buku, berbagai literatur, peraturan perundang-undangan serta melalui media elektronik (internet) yang mengeksplorasi berbagai aspek peraturan perundang-undangan terkait *cyber-crime*. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan *cyber law* di Indonesia.

ANALISIS DAN DISKUSI

Pengaturan Kejahatan Dunia Maya (*Cyber Crime*) dalam Hukum Positif di Indonesia

Cyber crime masih hangat diperdebatkan dikalangan sarjana hukum. Hal ini dikarenakan bentuk kejahatan ini relatif baru. Hukum pidana positif (KUHP dan KUHAP) telah dikritik dan dipertahankan karena kemampuannya menangani kejahatan ini. Penjahat dunia maya akan ditangkap oleh penegak hukum. *Cyber crime* masih tertangkap berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama yang memenuhi kriteria pasal-pasal atipikal KUHP. Ketika produk ini dianggap tidak cukup untuk mencegah berbagai bentuk kejahatan online, banyak instrumen hukum pidana di luar KUHP dapat digunakan untuk menyelesaikan kejahatan melalui penerapan teknologi ini. Instrumen-instrumen ini mencakup pendekatan yang berbeda terhadap undang-undang hukum yang berbeda.[7] Untuk mendalami bagaimana kejahatan dunia maya ditangani menurut hukum Indonesia, pertama-tama penelitiakan menganalisisnya dengan mempertimbangkan unsur-unsur kejahatan yang termasuk dalam KUHP. Para ahli telah menciptakan istilah "kejahatan dunia maya", dan akan mengusulkan berbagai kategori kriminalitas dunia maya, dengan mengingat bahwa istilah tersebut mencakup berbagai kegiatan.Kekerasan dalam rumah tangga, perdagangan orang, korupsi, kejahatan dunia maya, dan sebagainya adalah contoh kejahatan yang saat ini diatur oleh undang-undang yang terpisah dari KUHP. Jika undang-undang berikutnya yang mengatur perbuatan yang sama tidak menentukan unsur pidana, maka KUHP menjadi acuan untuk melihat unsur-unsur tersebut. Dalam hukum pidana, sesuatu yang dikatakan sebagai kejahatan apabila tindakan jahat tersebut dirumuskan dalam suatu delik atau tindak pidana, dan bagi pelanggarnya dapat dijatuhi pidana. Istilah tindak pidana atau *strafbaarfeit* di dalam bahasa Belanda ialah *Strafbaar* "dapat

[7] Irma yunita, M Kevin Ramadhan, and M Candra, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (Studi Kasus Phising Sebagai Ancaman Keamanan Digital)," *Jurnal Hukum Legalita* 5, no. 2 (2023): 143–55.

dihukum" dan *Feit* "sebagian dari suatu kenyataan''. Menurut beberapa ahli hukum dapat disebutkan sebagai berikut:[8]

1. Hazewinkel Suringa, *strafbaarfeit* merupakan suatu perilaku manusia yang pada suatu saat tertentu telah ditolak di dalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harusditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yangbersifat memaksa yang terdapat didalamnya.
2. Pompe, *strafbaarfeit* merupakan suatu tindakan yang menurut sesuatu rumusan Undang-undang telah dinyatakan sebagai tindakan yang dapat dihukum.
3. Simons, *strafbaarfeit* merupakan suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undangtelah dinyatakan sebagai suatu tindakan yang dapat dihukum.

Menurut Simons, bahwa *strafbaarfeit* dirumuskan sebagai berikut :

a. Untuk adanya suatu *strafbaarfeit* disyaratkan bahwa harus terdapat suatutindakan yang dilarang ataupun yang diwajibkan oleh undang-undang, dimana pelanggaran terhadap larangan atau kewajiban semacam itu telahdinyatakan sebagai suatu tindakan yang dapat dihukum;
b. Agar sesuatu tindakan itu dapat dihukum, maka tindakan tersebut harus memenuhi semua unsur dari delik seperti yang dirumuskan dalam undang-undang, dan
c. Setiap *strafbaarfeit* sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakansuatu tindakan melawan hukum atau merupakan suatu "*onrechtmatige handeling*"

Pada intinya bahwa suatu perbuatan yang dilakukan serta melawan hukum namun dilanggar oleh seseorang, maka perbuatan yang bersangkutan dapat dikenakan suatu sanksi pidana menurut suatu peraturan yang berlaku. *Cyber Crime* merupakan jenis baru dalam dunia kriminal. KUHP memilikiyurisdiksi yang jelas bahwa sesuai Pasal 2 KUHP menyebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu delik di Indonesia. Hal ini menurut saya menjadi hambatan dalam penegakan kejahatan siber (*cyber crime*) karena bisa jadi pelakunya melakukan kejahatan tersebut di luar Indonesia sedangkan korbannya

[8] P.A.F Lamintang. 1997. *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Citra Aditya Bakti

adalah orangIndonesia. Sedangkan apabila sebaliknya, negara kita seakan tidak mampu karena belum adanya perjanjian *mutual legal assistant* dalam bidang hukum pidana (ekstradisi). Penjelasan di atas merujuk pada definisi bahwa ruang *cyber* bersifat global,tidak terikat pada yurisdiksi nasional suatu negara. Hal ini karena *cyber space* tercipta melalui ruang internet. Pendapat bahwa *cyber crime* sama dengan *computercrime* terkadang tidak relevan lagi karena pelaku dapat menggunakan media atau alat lain dalam melakukan kejahatan tersebut.

Bentuk-bentuk *cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu :[7]

1. Delik-delik yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
   a. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
   b. *Data interference* (mengganggu data komputer)
   c. *System interference* (mengganggu sistem komputer)
   d. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
   e. *Misuse of devices* (menyalahgunakan peralatan komputer)
2. Delik-delik yang berhubungan dengan komputer : pemalsuan danpenipuan (*computer related offences; forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child phornography*).
4. Delik-delik yang berhubungan dengan hak cipta (*offences-related ofinfringements of copyright*).

Mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Namun, hukum pidana (KUHP) menurut sebagian berpendapat tidak dapat menjangkau kejahatan ini, sementara sebagian yang lain berpendapat bahwa hukum pidana positif

dapat menjangkau kejahatan ini.[9] Sedangkan pidana dalam UU ITE dalam Regulasi mengenai pemakaian Teknologi Informasi dan Komunikasi (TIK) sudah ditetapkan secara jelas setelah diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setelah itu mengalami pembaharuan menjadi Undang-Undang Nomor 19 Tahun 2016 serta mengalami pembaharuan lagi menjadi Undang-Undang Nomor 1 Tahun 2004 (disingkat UU-ITE). Beberapa tahun setelah UU-ITE kembali dilakukan pembaharuan, isu-isu seputar penggunaan TIK tidak lagi menjadi topik pembicaraan yang utama. Namun, dengan meningkatnya penggunaan internet di masyarakat, terutama dalam penggunaan media sosial, kasus-kasus terkait informasi serta transaksi elektronik juga semakin banyak terjadi khususnya mengenai lonjakan kasus-kasus terkait Undang-Undang ITE. Undang-undang No. 19 Tahun 2016 tentang Perubahan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan rincian tentang apa yang dinilai tidak sesuai dengan hukum. Melanggar UU ITE dapat mengakibatkan denda hingga hukuman penjara. Tindakan yang dilarang oleh Pasal 27 UU ITE, yaitu:

1. Memperluas Video Asusila
2. Judi Online
3. Melakukan Pencemaran Nama Baik
4. Pemerasan serta Pengancaman

Sedangkan dalam UU ITE pasal 28 dijabarkan sebagai berikut:

1. Berita Bohong
2. Ujaran Kebencian

Materi UU ITE terbagi dua, yaitu: pengaturan transaksi elektronik dan informasi elektronik hal ini sebagaimana dijelaskan dalam Undang-Undang Nomor 1 Tahun 2024 tentang UU ITE, serta pengaturan pelanggaran yang tak diperbolehkan dan diancam hukuman pidana (*cybercrime*). Selain itu, UU ITE adalah pengaturan tindak pidana siber pada Undang-Undang pertama di Indonesia.

Efektivitas Penegakan Hukum Terhadap Kejahatan Dunia Maya (Cyber Crime)

Kejahatan dunia maya (*cyber crime*) yang timbul akibat adanya kemajuan teknologi yang begitu pesat banyak mengakibatkan dampak negatif dan positif dari adanya teknologi tersebut.

[9] Agus Raharjo. 2002. *Cybercrime : Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi.* Bandung: PT. Citra Aditya Bakti

Dampak positif dapat berupa adanya e-mail, internet banking, serta hal-hal lain. Namun, perkembangan ini juga membawa pengaruh negatif yang dilakukan guna untuk memperoleh informasi atau data-data penting lainnya. Tindakan ini dilakukan tidak hanya semata-mata untuk mencari keuntungan dan menemukan titik lemah dari si target. Kejahatan ini dapat digolongkan lebih relatif baru jika dibandingkan dengan kejahatan konvensional lainnya. Meskipun kejahatan jenis ini telah muncul pada awal tahun 1961, ia tidak sepopuler kejahatan konvensional yang selalu mudah dijangkau oleh telinga masyarakat. Sekalipun telah lama ada, namun belum ada kesepahaman para ahli untuk memberikan definisi baik itu kejahatan dunia maya (*cyber crime*) maupun tindak pidana peretasan itu sendiri. Kendati demikian, telah banyak yang memakai istilah siber, kejahatan dunia maya, kejahatan firtual, dan bahkan tetap menggunakan istilah *cybercrime.*

Kejahatan dunia maya memang merupakan kegiatan kriminal yang berbeda yang memerlukan seperangkat aturan dan peraturannya sendiri di luar lingkup KUHP karena karakteristik unik dari teknologi yang berkembang pesat yang memungkinkannya, maka diperlukan semacam pengaturan luar biasa.Secara konseptual, putusan ini membutuhkan pengetahuan hukum (pidana) di Indonesia. Menurut Rene David, Indonesia memiliki “sistem hukum campuran”. Namun, warisan hukum kontinental tampaknya lebih penting dalam praktik dan pengembangan ilmu hukum dalam bidang hukum publik, khususnya hukum pidana. Oleh karena itu, pendekatan pembentukan aturan mengenai masalah *cyber crime* sebaiknya dilakukan secara terpadu dengan melakukan revisi atau perombakan keseluruhan KUHP.Oleh karena itu, setidaknya ada tiga hal yang harus diperhatikan dalam mengkriminalkankejahatan dunia maya.Pengaturan tindakan yang tergolong kejahatan dunia maya tidak boleh overkriminalisasi, karena akan berdampak negatif pada perkembangan teknologi komputer di bidang multimedia atau IT, yang sangat penting bagi negara Indonesia untuk menghadapi era globalisasi, yakni:(i) Hanya tindakan-tindakan yang benar-benar merugikan dan dapat menyebabkan akses yang serius harus dipilih (prinsip selektif dan terbatas), (ii) Apakah biaya penyusunan ketentuan yang mengatur kejahatan dunia maya yang tergolong kejahatan dunia maya yang rumit dan kompleks, biaya pemantauan dan penegakan ketentuan tersebut, yang membutuhkan fasilitas atau sarana berteknologi tinggi, dan beban yang harus ditanggung? ditanggung oleh korban akan diimbangi dengan akibat, yaitu keadaan hukum di dunia maya (prinsip cost and benefit), (iii) penting untuk memperhatikan kapasitas atau kemampuan tenaga kerja aparat penegak hukum di Indonesia yang akan diserahi tugas untuk menegakkan ketentuan yang mengatur mengenai tindak pidana komputer yang tergolong cyber crime, sehingga terdapat bukanlah beban yang tidak semestinya.

Adapun beberapa contoh tindakpidana *cyber crime* diantaranya sebagai berikut:

1. Pencurian (*Pasal 362)*

Ketentuan Pasal di atas dapat digunakan dalam kasus pencurian nomor kartukredit orang lain dengan menggunakan internet untuk melakukan transaksi.Setelah barang dikirimkan, penjual tidak dapat mencairkan uangnya karenapemilik kartu bukanlah orang yang melakukan transaksi.

2. Penipuan (*Pasal 378)*

Ketentuan pasal di atas dapat digunakan untuk kasus penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uangdikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3. Pemerasan dan Pengancaman (*Pasal 335)*

Ketentuan pasal di atas dapat digunakan dalam kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahuirahasia korban.

4. Pencemaran nama baik (*Pasal 311 ayat (1))*

Ketentuan Pasal di atas dapat digunakan pada Kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

5. Judi online (*Pasal 303 ayat (1) butir 1)*

Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* (ex: judi bola *online*) di Internet denganpenyelenggara dari Indonesia.

6. Pornografi (*Pasal 282)*

Dapat dikenakan untuk penyebaran pornografi maupun *website* porno yangbanyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran *domain* tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet, misalnya kasus terdahulu antara Sukma Ayu-B'jah dan kasus Ariel.

7. Hacking (*Pasal 406)*

Pasal di atas dapat digunakan pada kasus *deface* atau *hacking* yang membuatsistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

Dari beberapa contoh kasus yang dikaitkan dengan tindak pidana *cyber crime* maka sebenarnya masih terdapat beberapa kekurangan dalam upaya penegakan hukumnya. Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang pertama di bidang Teknologi Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pendahulu yang meletakkan dasar pengaturan di bidang pemanfaatan teknologi informasi dan transaksi elektronik. Akan tetapi dalam kenyataannya, perjalanan implementasi dari UU ITE mengalami persoalan-persoalan. Kemudian Undang-undang No. 19 Tahun 2016 UU ITE membahas tentang perubahan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada beberapa pasal kemudian dirubah untuk kedua kalinya dengan Undang-undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang ITE. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Upaya penanggulangan kejahatan tersebut dapat berupa upaya preventif dan upaya represif yaitu sebagai berikut:[10]

1. Upaya preventif

Upaya ini merupakan upaya pencegahan yang dilakukan guna mencegah timbulnya suatu kejahatan didalam lingkup masyarakat. Beberapa hal yang dapat dilakukan guna mencegah terjadinya suatu kejahatan adalah dengan melakukan edukasi terhadap masyarakat, melakukan pemblokiran, membentuk Badan Siber dan Sandi Negara (BSSN).

2. Upaya represif

Upaya ini merupakan salah satu upaya yang bersifat konsepsional, dimana upaya ini dilakukan setelah terjadinya suatu kejahatan. Upaya ini bertujuan untuk menindak pelaku

[10] Amir Ilyas dan A.S. Alam. 2018. *Kriminologi Suatu Pengantar*. Jakarta: Kencana.

kejahatan seperti penjatuhan sanksi atau penjatuhan pidana sesuai dengan pelanggaran yang telah dilakukan.

Di Indonesia aparat penegak hukum yang memiliki kewenangan dalam menangani perkara tindak pidana *cyber crime* dibagi menjadi 3 yaitu ;

1. Pengadilan

Pengadilan sebagai instansi resmi negara bertugas untuk melakukan pemeriksaan, memberikan keadilan dengan cara mengadili, memberikan putusan, dan menyelesaikan segala perkara atau permasalahan yang diajukan oleh warga masyarakat. Perkara yang diselesaikan melalui pengadilan akan dapat berjalan sebagaimana mestinya jika semua pihak yang berada atau ikut didalam penyelesaian perkara tersebut. Para pihak yang berperkara atau dari hakimnya sendiri harus mengikuti aturan main (*rule of game*) secara jujur dan sesuai dengan peraturan yang ada. Pihak yang mengajukan perkara di pengadilan tentunya mempunyai maksud untuk mendapatkan penyelesaian dan pemecahan perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan (*justiciabellen*). Untuk mendapatkan penyelesaian perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan harus melalui proses pembuktian. Proses tersebut bertujuan untuk mengetaui duduk perkara secara jelas, yaitu peristiwa yang benar dan peristiwa yang salah. Di dalam proses pembuktian para pihak diberikan kesempatan untuk mengemukakan pendapat mengenai peristiwa yang terjadi. Hal tersebut sangat penting karena sebagai dasar untuk meneguhkan hak dan membantah hak dari pihak lain. Dalam hal mengemukakan pendapat para pihak tidak cukup sekedar memberikan pendapatnya secara lisan maupun tertulis saja, tetapi harus didukung dan disertai dengan bukti-bukti yang sah menurut hukum agar kebenarannya dapat dipastikan.[11]

2. Kejaksaan

Kejaksaan memiliki tugas utama sebagai salah satu lembaga penegak hukum dalam system peradilan pidana Indonesia. Adapun tugasnya untuk melakukan penuntutan dan sebaliknya. Penuntutan merupakan kewenangan satu-satunya yang hanya dimiliki oleh

[11] Soerjono Soekanto. 1990. *Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum*. Bandung: Mandar Maju

kejaksaan dan tidak dimiliki oleh Lembaga penegak hukum lain. Dalam melaksanakan fungsi, tugas, dan wewenangnya, kejaksaan terlepas dari segala pengaruh kekuasaan pemerintah, dan pengaruh dari kekuasaan lainnya. Negara memberikan jaminan kepada jaksa di dalam menjalankan profesinya tanpa adanya intimidasi, gangguan, godaan, dan campur tangan yang tidak sesuai atau pembeberan dari segala sesuatu yang belum teruji kebenarannya, baik terhadap pertanggungjawaban perdata, pidana, maupun lainnya.[12]

3. Kepolisian

Penindakan kasus *cyber crime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan computer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana. Penegakan hukum disini tidak hanya memperhatikan pendekatan kepastian hukum tetapi juga harus memperhatikan pendekatan keadilan dan kemanfaatan hukum sebagaimana tujuan hukum itu sendiri.[13] Dengan demikian dapat dipahami bahwa efektivitas hukum dapat dilihat seberapa besar ketaatan masyarakat terhadap hukum.[14]

Adapun perbuatan yang dilarang dalam kaitannya dengan tindak pidana teknologi informasi artinya yang dilakukan dengan melawan hukum dan tanpa hak telah diatur di dalam hukum nasional, yaitu:

1. KUHP dan KUHAP
2. Undang-Undang No. 16 Tahun 2016 Tentang Informasi dan Transaksi Elektronik:

---

[12] Andri Winjaya Laksana, "Tinjauan Hukum Pemidanaan Terhadap Pelaku Penyalahguna Narkotika Dengan Sistem Rehabilitasi," *Jurnal Pembaharuan Hukum* 2, no. 1 (2016): 74-85.

[13] Renny N.S. Koloay, "Perkembangan Hukum Indonesia Berkenaan Dengan Teknologi Informasi Dan Komunikasi," *Jurnal Hukum Unsrat* 22, no. 5 (2016): 16–27.

[14] Atang Hermawan Usman, "Kesadaran Hukum Masyarakat Dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum Di Indonesia," *Jurnal Wawasan Hukum* 30, no. 1 (2014): 26–53.

a. Pasal 27 ayat (1) melarang perbuatan yang memanfaatkan teknologi informasi yang bermuatan kesusilaan, ayat (2) yang bermuatan perjudian, ayat (3) yang bermuatan pencemaran nama baik, ayat (4) yang bermuatan pemerasan dan/atau pengancaman.
b. Pasal 28 ayat (1) "melarang perbuatan yang memanfaatkan teknologi informasi yang mengakibatkan kerugian konsumen dalam transaksi elektronik", ayat (2) menimbulkan kebencian yang bermuatan unsur SARA.
c. Pasal 29 "melarang perbuatan yang memanfaatkan teknologi informasi yang bermuatan ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
d. Pasal 30 ayat (1) "melarang perbuatan yang memanfaatkan teknologi informasi untuk mengakses computer dan/atau system elektronik milik orang lain", ayat (2) "dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, ayat (3) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".
e. Pasal 31 ayat (1) "melarang intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain", ayat (2) "yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan".
f. Pasal 32 ayat (1) "melarang dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik public", ayat (2) "memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak".
g. Pasal 33 "melarang perbuatan yang menyebabkan terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya".
h. Pasal 34 "melarang memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau

perangkat lunak komputer untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33".

i. Pasal 35 "melarang melakukan manipulasi, dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik".

KESIMPULAN

Pengaturan kejahatan dunia maya (*cyber crime*) dalam hukum positif di Indonesia merupakan tindak pidana yang menggunakan sarana atau bantuan dari Sistem Elektronik. Semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik dapat masuk dalam kategori tindak pidana cyber crime. Efektivitas Penegakan Hukum Terhadap Tindak Pidana cyber crime telah di laksanakan berdasarkan Kitab Undang-Undang Hukum Pidana dan Undang– Undang Nomor 1 tahun 2024 Tentang Informasi dan Transaksi Elektronik. Namun, dalam hal pelaksanaan di lapangan mengalami kendala yang berasal dari aparat penegak hukumnya sendiri. Seperti pihak kepolisian yang minim akan keahlian mengenai (IT), fasilitas dan sarana yang kurang memadai. Sehingga dari data penelitian tersebut di dapatkan kasus-kasus kejahatan online menjadi kasus yang paling sering terjadi karena pelaku yang tidak diketahui identitasnya menyebabkan kepolisian mengalami kendala dalam melacak akun–akun tersebut sehingga dapat di katakan bahwa penegakan hukum dalam hal tindak pidana siber belum efektif

DAFTAR PUSTAKA

A.S. Alam dan Amir Ilyas. 2018. ***Kriminologi Suatu Pengantar***. Jakarta: Kencana

Agus Raharjo. 2002. ***Cybercrime : Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi***. Bandung: PT. Citra Aditya Bakti

Ashady, S Januar. 2024. **"Cybercrime Sebagai Kejahatan Dunia Maya Dalam Perspektif Hukum Dan Masyarakat."** *Jurnal Jurisdische* 1(2)

Dwi, Putro Widodo. 2019. **"Pancasila Di Era Paska Ideologi."** *Jurnal Veritas et Justitia* 5(1)

Irma yunita, M Kevin Ramadhan, dan M Candra. 2023. **"Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (Studi Kasus Phising Sebagai Ancaman Keamanan Digital)."** *Jurnal Hukum Legalita* 5(2)

Johnny Ibrahim. 2005. ***Teori Dan Metode Penelitian Hukum Normatif*.** Jakarta: Bayumedia Publishing

Koloay dan Renny N.S. 2016. **"Perkembangan Hukum Indonesia Berkenaan Dengan Teknologi Informasi Dan Komunikasi."** *Jurnal Hukum Unsrat* 22(5)

Laksana, Andri Winjaya. 2016. **"Tinjauan Hukum Pemidanaan Terhadap Pelaku Penyalahguna Narkotika Dengan Sistem Rehabilitasi."** *Jurnal Pembaharuan Hukum* 2(1)

Muslimah. 2021. **"Kajian Filsafat Ilmu Dalam Kebudayaan."** Bangun Kaprima : Jurnal Pengembangan Rekayasa Sosial Dan Humaniora 7(2)

P.A.F Lamintang. 1997. ***Dasar-Dasar Hukum Pidana Indonesia.*** Bandung: Citra Aditya Bakti

Peter Mahmud Marzuki. 2017. ***Penelitian Hukum***. Jakarta: Prenada Media

Pribadi, Insan. 2018. **"Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana."** *Jurnal Lex Renaissance* 3(1)

Soerjono Soekanto. 1990. ***Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum)***. Bandung: Mandar Maju

Usman, Atang Hermawan. 2014. **"Kesadaran Hukum Masyarakat Dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum Di Indonesia"**. *Jurnal Wawasan Hukum* 30(1)