ISSN 2541-6502
E-ISSN 2776-9844

AKTUAL JUSTICE
JURNAL ILMIAH MAGISTER HUKUM
PASCASARJANA UNIVERSITAS NGURAH RAI

PERANAN CYBER LAW DALAM PENEGAKAN HUKUM TERHADAP TINDAK PIDANA DUNIA MAYA (CYBER CRIME)

I Gusti Bagus Agung Kusuma Atmaja
Institut Teknologi Dan Bisnis STIKOM Bali, Email : agungkusumaatmaja85@gmail.com

Abstract

The activities people do nowadays are mostly carried out in cyberspace. This can cause positive and negative effects such as cybercrime. The research method used in this study is the normative juridical research method, where this normative juridical research is literature law research carried out by examining literature materials. Cyber crime today is very diverse in form such as phishing, hacking, cyber stalking and cyber bullying. The regulations related to handling cyber crime include the Criminal Code, Law Number 3 of 2011 concerning Fund Transfer, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Keywords: *criminal law, cyber law, cyber crime.*

Abstrak

Kegiatan sebagian besar manusia saat ini banyak dilakukan di dunia maya, tentunya ini dapat menimbulkan efek positif maupun negatif seperti tindak pidana dunia maya. Metode penelitian yang digunakan di dalam penelitian ini yaitu metode penelitian yuridis normatif. Dimana penelitian yuridis normatif ini adalah penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan kepustakaan. Kejahatan dunia maya (cyber crime) saat ini sangat beragam bentuknya seperti penipuan *Phising,* peretasan, *cyber stalking* maupun *cyber bullying*. adapun peraturan-peraturan yang terkait dengan penanganan tindak pidana dunia maya (cyber crime) antara lain Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana, Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata Kunci: *hukum pidana, cyber law, cyber crime.*

1. Pendahuluan

Dewasa ini, di negara manapun di dunia ini sangat memiliki ketergantungan akan kehadiran serta peran dari teknologi informasi. Peran dari teknologi informasi ini tidak dapat dipungkiri, mengingat segala sesuatunya lebih dipermudah karena kehadirannya, seperti dalam mengirimkan surat, sekarang sudah lebih mudah dengan adanya email, mengakses berita tidak lagi dengan surat kabar atau koran tapi saat ini sudah bisa melalui media-media online, sehingga lebih mudah dan praktis.

Kehadiran teknologi informasi ini selain memberikan kemudahan tentunya juga ada masalah yang dapat ditimbulkan. Sebagai sebuah gejala sosial,kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern)[1]. Efek negatif dari perkembangan teknologi informasi ini tentunya dapat mengganggu kehidupan sosial maupun pribadi dari setiap manusia, karena ada berbagai macam modus kejahatan yang dapat dilakukan di dunia maya saat ini. Modus kejahatan-kejahatan yang dapat terjadi ini antara lain penipuan *Phising,* peretasan, *cyber stalking,* judi online, pornografi sampai dengan adanya *cyber bullying.* Disini peranan maupun kehadiran negara sangat diperlukan, dimana kehadiran negara ini berupa dibuatkannya peraturan perundang-undangan yang dapat melindungi seluruh warga negara sehingga dapat memberikan rasa aman disaat mengakses atau menggunakan media teknologi informasi tersebut. Hkum pidana sebagai pengendalian sosial juga dapat dimanfaatkan keberadaannya untuk menanggulangi kejahatan yang terjadi berupa pelanggaran norma-norma yang berhubungan dengan pemanfaatan teknologi informasi yang berpotensi akan terjadinya tindak kriminal, guna memberikan perlindungan serta rasa aman kepada masyarakat dari bahaya kejahatan tersebut.

Harapan dari masyarakat akhirnya direalsisasikan oleh pemerintah dengan diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang ini memiliki dua tujuan utama :

[1]Agus Raharjo. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan berteknologi Tinggi.* Citra Aditya Bakti. Bandung.

Pertama, adalah untuk memfasilitasi perkembangan ekonomi digital di Indonesia. Kedua, untuk memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara internet di Indonesia.[2]

Dengan diberlakukannya undang-undang ini, tentunya pemerintah berharap agar pengguna internet di Indonesia lebih merasa aman dan lebih bijak di dalam penggunaan internet untuk tujuan yang tentunya memberikan dampak positif dan juga mempermudah serta membantu masyarakat dalam melakukan segala hal yang berhubungan dengan dunia maya.

2. Metode Penelitian

Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif. Penelitian hukum yuridis normatif ini dapat disebut juga sebagai penelitian hukum doktrinal. Hukum dikonsepsikan sebagai apa yang tertulis di dalam peraturan perundang – undangan atau hukum yang dikonsepsikan sebagai kaidah atau norma yang merupakan patokan berperilaku masyarakat terhadap apa yang dianggap pantas.

Pendekatan yang dipergunakan adalah pendekatan perundang-undangan (*Statute Approach*) dan pendekatan konseptual (*Conceptual Approach*). Penulis mengkaji Undang-Undang mengenai cyber law sedangkan Bahan Hukum yang dipergunakan adalah bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundang-undangan yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.[3]

3. Hasil Dan Pembahasan

[2]Soemarmo Partodihardjo. (2009). *Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transasksi Elektronik*. PT. Gramedia Pustaka Utama. Jakarta.

[3]Soerjono Soekanto dan Sri Marmudji. (2001). *Peneltian Hukum Normatif*. Raja Grafindo Persada. Jakarta.

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

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 harus ditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yang bersifat 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-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.[4]

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 (*cyber crime*) dalam arti luas.

Dalam beberapa pandangan ahli, terdapat perbedaan dalam menafsirkan tentang cyber crime. Muladi dalam "Bunga Rampai Hukum Pidana" berpendapat bahwa sudut pandang cyber crime adalah dengan menggunakan pendekatan computer crime. Namun adapula yang berpendapat bahwa sebenarnya cyber crime berbeda dengan computer crime. Walaupun demikian, sesungguhnya memang ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala

[4] P.A.F Lamintang. (2007). *Dasar-dasar Hukum Pidana Indonesia*. Citra Aditya Bakti. Bandung.

kejahatan di internet dengan peralatan apapun, seperti pengertian komputer dalam The Proposed West Virginia Computer Crimes Act:

"data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similiar device."

Terjemahan bebasnya : peralatan pemrosesan data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau *tipe-setter*, sebuah kalkulator tangan atau peralatan serupa lainnya.[5]

Mengikuti perkembangan zaman pada masa sekarang ini, dalam menanggulangi serta mencegah terjadinya *cyber crime,* maka telah diterbitkan peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Informasi dan Transaksi Elektronik ini sangat diharapkan dapat menjadi kekuatan untuk mengendalikan serta dan melakukan penenetiban dalam rangka kegiatan-kegiatan terkait dengan pemanfaatan teknologi informasi tersebut.

Menurut Widodo, bahwa *cybercrime* diartikan sebagai kegiatan seseorang, sekelompok orang, badan hukum yang memakai komputer bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran (target). Beberapa tipe kejahatan yang sering terjadi di Internet yaitu:

1. *Illegal acces/Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem komputer dan jasa), adalah suatu bentuk kejahatan yang dilakukan dengan cara merentas atau memasuki/menyusup ke dalam suatu sistem

[5]Abdul Wahid dan Mohammad Labib. (2005). *Kejahatan Mayantara (cyber crime)*. Refika Aditama. Bandung.

jaringan komputer secara tidak sah, atau tanpa izin atau tanpa sepengetahuan dari si pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal Contents.* Merupakan suatu modus kejahatan cybercrime dengan cara memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Data Forgery.* Adalah modus kejahatan dalam dunia maya yang dilakukan dengan cara memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolaholah terjadi "salah pengetikan" yang pada akhirnya akan menguntungkan si pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit yang patut diduga akan disalah gunakan oleh si pelaku.
4. *Cyber Espionage (Spionase Cyber)* Adalah suatu kejahatan yang modusnya menggunakan jaringan internet, untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer (computer network system) pihak yang menjadi sasarannya.
5. *Cyber Sabotage and Extortion (Sabotase dan Pemerasan Dunia Maya).* Dalam kejahatan ini modus yang dilakukan biasanya dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan komputer yang terhubung dengan internet. Dimana, biasanya kejahatan ini dilakukan dengan cara menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan namun telah dikendalikan sesuai yang diinginkan oleh si pelaku.
6. *Offense Against Intellectual Property (Pelanggaran Terhadap Hak atas Kekayaan Intelektual*). Kejahatan ini modus operandinya ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai suatu

contoh; peniruan tampilan pada suatu web page situs milik orang lain secara illegal.

7. *Infringements of Privacy (Infringements privasi).* Modus pada kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain, maka dapat merugikan korban secara materiil maupun immaterial, seperti bocornya nomor kartu kredit, nomor PIN ATM, dan lain sebagainya.[6]

Di Indonesia sendiri, tindak pidana yang dilakukan di dunia maya (*cybercrime*) telah diatur dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ada berbagai jenis tindak pidana dunia maya tersebut, antara lain sebagai berikut:

1. Tindakan yang melanggar kesusilaan.

   Pada Pasal 27 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum". Namun perbuatan membagikan/ menyebarkan/membuat konten informasi elektronik/dokumen elektronik yang melanggar kesopanan (kesusilaan) tidak dijelaskan dengan sendirinya dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelanggaran etika/kesusilaan melalui media internet sendiri merujuk pada KUHP. Dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, dalam Pasal 27 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun

[6]Antoni. (2017). *Kejahatan Dunia Maya (Cybercrime) dalam Simak Online*. Jurnal Nuraini , 17 No.2, 261-274.

2008 tentang Informasi dan Transaksi Elektronik mengatur tentang informasi dan transaksi elektronik, termasuk pornografi online dan prostitusi online. Jika kejahatan ini dilakukan terhadap anak-anak, maka akan menjadi semakin serius. Salah satu permasalahan yang diakibatkan oleh perkembangan teknologi informasi melalui jaringan internet adalah banyaknya situs yang menampilkan adegan porno. Tampaknya saat ini, sangat sulit melindungi Internet dari gangguan pedagang hiburan yang menjual pornografi.[7]

2. Perjudian

   Perjudian online diatur pada Pasal 27 ayat (2) Undang-undang Informasi dan Transaksi Elektronik. Dalam peraturan ini juga sama disebutkan bahwa: "Setiap orang dengan sengaja dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan perjudian".

3. Penghinaan atau pencemaran nama baik

   Pencemaran nama baik ataupun penghinaan di dunia maya merupakan larangan yang diatur pada Pasal 27 ayat (3) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008, yang berbunyi : "Setiap Orang dengan sengaja, dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan penghinaan atau pencemaran nama baik." Pembuat undang-undang menyamakan antara penghinaan dan pencemaran. Penghinaan sendiri ialah sebuah perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran. Kejahatan penghinaan terdiri dari penghinaan umum dan penghinaan khusus. Penghinaan umum mengacu pada obyek harga diri dan derajat orang pribadi, termasuk juga pencemaran. Sedangkan penghinaan khusus mengacu pada penghinaan yang memiliki obyek harga diri, kehormatan dan nama baik terbuka (umum).[8]

4. Pemerasan atau pengancaman

[7] *Ibid.*

[8] Adami Chazawi. (2013). *Hukum Pidana Positif Penghinaan*. Bayumedia Publishing. Malang.

Pada Pasal 27 ayat (4) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang No. 11 Tahun 2008 melarang pemerasan atau pengancaman di dunia maya. Dalam pasal tersebut dijelaskan: "Setiap orang yang 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 368 (1) KUHP mencantumkan kualifikasi perbuatan yang terhitung pemerasan atau pengancaman, yaitu: "Setiap orang yang bermaksud untuk menguntungkan dirinya sendiri atau orang lain secara melawan hukum (ilegal), memaksa seseorang untuk memberikan sesuatu milik orang tersebut maupun orang lain secara keseluruhan maupun sebagian dengan kekerasan maupun ancaman kekerasan atau menciptakan hutang maupun menghapus hutang, akan dihukum karena pemerasan dan dapat dijatuhi hukuman hingga 9 tahun penjara."

5. Penguntitan (*cyberstalking*)

   Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 Pasal 29 mengatur bahwa: "Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi". Ketentuan mengenai informasi dan transaksi elektronik dalam Pasal 29 mengatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan ketakutan, termasuk kata-kata atau tindakan tertentu. Ketentuan tersebut serupa dengan pengaturan cyberstalking di Amerika Serikat, Kanada, Inggis dan negara lainnya. Tindakan ini dilakukan dengan memanfaatkan teknologi informasi dan komukasi, semisal dengan mail bombs, unsolicited hate mail, obsence or threatening email, dan yang lainnya. [9]

6. Penyebaran berita palsu (*hoax*)

[9]Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama. Bandung.

Penyebaran berita palsu diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 Pasal 28 ayat (1), berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong/palsu serta menyesatkan, yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

7. Ujaran kebencian

   Pasal 28 ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentang pidana tersebut, yang berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang dirancang untuk menimbulkan kebencian atau permusuhan individu/ kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA)".

8. Akses ilegal

   Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik., dalam Pasal 30 mengatur sebagai berikut:

   a. Siapapun yang dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik orang lain dengan cara apapun.
   b. Siapapun dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses (membuka) Komputer atau Sistem Elektronik dengan cara apapun dengan maksud untuk memperoleh Informasi Elektronik atau Dokumen Elektronik.
   c. Siapapun yang melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik."

Dengan adanya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tentunya akan memberikan rasa aman kepada Masyarakat pengguna

teknologi informasi itu sendiri, dan tentunya pelaku tindak pidana di dunia maya akan berpikir saat ingin menjalankan niatnya untuk melakukan suatu tindak pidana. Karena seluruh perbuatan yang memenuhi unsur suatu kejahatan didunia maya telah diatur oleh pemerintah dan tentunya akan ada sanksi dari tindak pidana tersebut.

Tindak pidana peretasan yang diatur dalam pasal 30ayat (1),(2),dan (3) mengandung unsur sebagai berikut :

Pasal 30 ayat (1) UU ITE: "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun". Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses komputer dan/ atau sistem elektronik milik orang lain, serta unsur dengan cara apapun.

a. Unsur setiap orang Dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggungjawab dan cakap hukum berdasarkan atas Perundang-Undangan.
b. Unsur dengan sengaja dan tanpa hak melawan hukum Unsur ini merujuk pada niat atau kesengajaan dan penuh dengan keasadaran dari orang tesebut dalam melakukan suatu tindakan yang malawan hukum.
c. Unsur mengakses komputer dan/ atau sistem elektronik milik orang lain Unsur ini memberi gambaran bahwa sistem elektronik milik orang lain itu berarti hal yang bersifat pribadi milik orang lain dan bukan bersifat untuk umum.
d. Unsur dengan cara apapun Dengan cara apapun yang dimaksud dalam hal ini adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.[10]

Disebutkan dalam pasal 30 ayat 1 ini setiap orang dilarang secara tegas masuk kedalam sistem elektronik milik orang lain yang bersifat privasi atau pribadi. Sanksi pidanayang dapat menjerat pelaku peretasan tersebut telah diatur secara jelas dalam pasal 46 ayat 1 yakni "setiap orang yang memenuhi usnur sebagaimana dimaksud

[10]I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha. (2020). *Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)*. Jurnal Kontruksi Hukum, Vol. 1, No. 2.

dalam pasl 30 ayat (1),dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp.600.000.000,00(enam ratus juta rupiah).

Pasal 30 ayat (2) UU ITE: "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh infromasi elektronik dan/ atau dokumen elektronik". Dalam pasal 30 ayat (2) ini memiliki unsur yang sama seperti pada pasal 30 ayat (1),namun ayat (2) terdapat unsur memperoleh informasi elektronik dan/ atau dokumen elektronik, hal tersebut berarti orang yang mencoba masuk kedalam sistem tersebut memilikitujuan untuk mencuri suatu data atau informasi elektronik yang terdapat dalam sistem milik korban.

Pasal 30 ayat (2) ini berkaitan langsung dengan pasal 46 ayat (2) mengenai ancaman pidana jika melanggar ketentuan pasal 30 ayat (2): "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah)".

Unsur dalam pasal 30 ayat (3) terdapat unsur dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Unsur ini memberi indikasi bahwa pelaku peretasan atau hacker melakukan tindakan tersebut dengan cara menerobos sistem keamanan komputer tersebut. Untuk sanksi pidananya sendiri telah diatur dalam pasal 46 ayat (3) dimana untuk pelanggaran tersebut dikenakan hukuman kurungan penjara seberat-beratnya 8 (delapan) tahun dan/atau membayar denda sebanyak-banyaknya Rp.800.000.000,00 (delapan ratus juta rupiah). Pemberatan penjatuhan pidana bagi pelaku peretasan berdasarkan atas objek dan subjek dari tindak pidana yang bersangkutan, yaitu:

1. Berdasarkan objek tindak pidana peretasan atau hacking
   a. Pasal 52 ayat (2) UU ITE Dalam pasal ini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.

b. Pasal 52 ayat (3) UU ITE Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara.

2. Berdasarkan objek tindak pidana peretasan atau hacking
   a. Pasal 52 ayat (2) UU ITE

      Dalam pasalini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistemelektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.
   b. Pasal 52 ayat (3) UU ITE

      Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara.
3. Berdasarkan atas subjek tindak pidana peretasan atau hacking Pasal 52 ayat (4) UU ITE, pemberatan dapat dijatuhkan apabila terbukti bahwa peretasan tesebut dilakukan oleh korporasi.

Dalam hal penghinaan terhadap seseorang secara sengaja yang dilakukan di dunia maya dapat dikategorikan sebagai pencemaran nama baik terhadap seseorang. Di dalam Kitab Undang-Undang Hukum Pidana, ada 6 (enam) jenis penghinaan yaitu Menista/*smaad* (pasal 310 KUHP), Memfitnah/*laster* (Pasal 311 KUHP), Penghinaan Ringan/*envoundige belediging* (Pasal 315), Mengadu Dengan Memfitnah/*lasterlijke* (Pasal 317), menyuruh dengan memfitnah/*lasterlijke verdachtmaking* (Pasal 318). Sedangkan di dalam Undang-Undang Informasi dan Transaksi Elektronik mengatur tentang perbuatan seseorang yang mencemarkan nama baik yang berlaku pada setiap warga baik berada di Indonesia maupun diluar daerah. Sanksi bagi seseorang yang melakukan pencemaran nama baik ada pada pasal 23 ayat (3) di denda maksimal 1 miliyar rupiah.

4. Kesimpulan

Saat ini di Indonesia telah memiliki peraturan yang mengatur mengenai segala aktifitas di dunia maya yakni ada dalam Undang-Undang Nomor 1 Tahun 2024

tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dimana di dalam undang-undang ini telah mengatur mengenai segala jenis kegiatan maupun transaksi yang dilakukan melalui media internet. Selain itu, di dalam undang-undang ini juga mengatur mengenai sanksi-sanksi yang dapat dijatuhkan apabila terjadi pelanggaran terhadap undang-undang ini. Peranan undang-undang ITE saat ini sangat diharapkan dapat memberi rasa aman kepada masyarakat pengguna internet atau teknologi informasi.

Daftar Pustaka

BUKU

Abdul Wahid dan Mohammad Labib. (2005). *Kejahatan Mayantara (cyber crime).* Refika Aditama. Bandung.

Adami Chazawi. (2013). *Hukum Pidana Positif Penghinaan.* Bayumedia Publishing. Malang.

P.A.F Lamintang. (2007). *Dasar-dasar Hukum Pidana Indonesia.* Citra Aditya Bakti. Bandung.

Soemarmo Partodihardjo. (2009). *Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transasksi Elektronik*. PT. Gramedia Pustaka Utama. Jakarta.

Agus Raharjo. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan berteknologi Tinggi.* Citra Aditya Bakti, Bandung.

Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama. Bandung.

Soerjono Soekanto dan Sri Marmudji. (2001). *Peneltian Hukum Normatif*. Raja Grafindo Persada. Jakarta.

JURNAL

Antoni. (2017). *Kejahatan Dunia Maya (Cybercrime) dalam Simak Online*. Jurnal Nuraini, 17 No.2, 261-274.

I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha. (2020). *Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)*. Jurnal Kontruksi Hukum, Vol. 1, No. 2.

Yuni Fitriani dan Roida Pakpahan. (2020). *Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace.* Cakrawala : Jurnal Humaniora 20, no. 1.

PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kitab Undang-Undang Hukum Pidana (KUHP).