E-ISSN (2654-9026)
P-ISSN (1693-9891)

UPAYA PENAL DAN NON PENAL DALAM MENANGGULANGI TINDAK PIDANA TEKNOLOGI INFORMASI

Dwikari Nuristiningsih
Ependi
Fakultas Hukum Universitas Prof. Dr. Hazairin, S.H
Email Korespodensi: dwikarinuristiningsih898@gmail.com

Abstrak

Cybercrime dapat dilakukan melalui system jaringan komputernya itu sendiri yang menjadi sasaran dan komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan, oleh karena itu harus diantisipasi dengan hukum yang mengaturnya yang didalamnya dimana salah satunya mengatur ketentuan pidana, meskipun sudah ada perangkat hukum dan Undang-undang Nomor: 11 Tahun 2006 Tentang Informasi dan Transaksi dan Undang-undang Nomor : 19 Tahun 20016 Tentang Perubahan Atas Undang-undang Nomor: 11 Tahun 2016. Diantara fakta-fakta kejahatan dunia maya (*Cyber Crime*) Di Indonesia diantaranya adalah. pencurian data Bank Syariah Mandiri , Pembobolan data Kominfo, peretasan Website Kejagung RI, dll. Dalam penelitian ini yang menjadi permasalahan adalah upaya hukum penal saat ini mempunyai keterbatasan dalam melakukan penegakan hukum oleh karena itu harus diimbangi dengan upaya non penal yang bersifat preventif atau pecegahan yang harus dilakukan dalam menanggulangi tindak pidana Teknologi Informasi. Metode penelitian yang digunakan dalam penelitian ini adalah jenis penelitian yuridis normatif, dengan pendekatan perundang-undangan dan konseptual. jenis dan sumber datanya menitikberatkan pada data sekunder, Teknik pengumpulan data dengan melakukan penelitian kepustakaan.

Kata Kunci: Upaya Penal; Upaya Non Penal; Tindak Pidana Teknologi Informasi.

Abstract

Cyber crime can be carried out through the computer network system itself which is the target and the computer itself which is the means for committing the crime. Therefore, it must be anticipated by the law that regulates it, one of which regulates criminal provisions, even though there are already legal instruments and law number 11 of 2008 concerning electronic information and transactions. Among the facts about cyber crime in Indonesia include theft of Bank Syariah Mandiri data, hacking of Kominfo data, hacking of the website of the Attorney General of the Republic of Indonesia and others. In the research, the problem is that current penal efforts have limitations, therefore they must be balanced with non-penal efforts which are preventive or precautionary in nature which must be carried out in dealing with information technology crimes. The research method used in this research is a normative juridical type with a statutory and conceptual approach, the type and source of data focuses on secondary data, the data collection technique is by conducting a library study.

Keywords: *Non-Penal Measures; Penal Measures; Information Technology Crimes.*

I. Latar Belakang

Manusia adalah makhluk ciptaan Tuhan Yang Esa yang sempurna yang sangat berbeda dengan makhluk ciptaan lain nya. Manusia berkembang secara dinamis, dan dalam menjalani kehidupannya manusia sangat membutuhkan manusia yang lain atau orang lain, atau manusia adalah sebagai makllhuk sosial, baik dalam berinteraksi, berkomunikasi, bergaul maupun dalam memenuhi kebutuhan-kebutuhan hidupnya.

Seiring dengan perkembangan hubungan antara manusia yang satu dengan yang lain, pastilah aakan menuimbulkan suatu sengketa atau permasalahan diantara mereka, akan tetapi disisi lain lagi keberadaan manusia sebagai manusia yang berkembang secara dinamis akan menentukan juga perkembangan ilmu pengetahuan dan teknologi.

Di era global ini berbagai hal positif yang bisa dimanfaatkan oleh setiap bangsa terutama bidang teknologi, kemajuan teknologi juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bukan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola modernitas yang gagal mengedepankan prinsip humanitas, tetapi juga munculnya kejahatan di alam maya yang telah menjadi realitas dunia.

Memang tidak bisa diingkari oleh siapapun, bahwa teknologi itu dapat menjadi alaf perubahan di tengah masyarakat. Demikian pentingnya fungsi teknologi , hingga sepertinya masyarakat dewasa ini sangat tergantung dengan teknologi, baik untuk hal-hal positif maupun negatif. Pada perkembangannya internet juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak akan terpikirkan terjadi. Sebuah teori menyatakan bahwa crime is product of society it self, yang secara sederhana dapat diartikan bahwa semakin canggih tingkat intelektualitas suatu masyarakat maka akan semakin canggih dan beraneka ragam pulalah tingkat kejahatan yang dapat terjadi.

Salah satu contoh terbesar saat ini adalah kejahatan maya atau biasa disebut “cybercrime” (tindak pidana mayantara), merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Beberapa sebutan diberikan pada jenis kejahatan baru ini dai dalam berbagai tulisan , antara lain: sebagai “kejahatan dunia maya “(cyberspace/virtual-space offence), dimensi baru dari “hi-tech crime”, dimensi baru dari “transnational crime”, dan dimensi baru dari “white collar crime”.

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara secara global. Perkembangan teknologi informasi dan kominikasi telah pula menyebabkan perubahan dunia menjai tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum,.

Saat ini telah lahir suatu rezim hukum baruyang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau cyberlaw , secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaataan teknologi informasi dan komunikasi, Demikian pula hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law) dan hukum mayantara . Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem computer dan sistem komunikasi baik dalam lingkup local maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem computer yang merupakan sistem elektronik yang dapat dilihat secara virtual .

Pentingnya penegakan hukum terhadap penyalahgunaan media sosial untuk menyebar kebencian dan fitnah menjadi kebutuhan utama dalam karena kejahatan ini sudah tergolong parah, jika dilihat dari perspektif hukum , sosial budaya, politik, pembangunan ekonomi, hak asasi manusia dan keamanan cbyer.

Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan : Manusia adalah makhluk ciptaan Tuhan Yang Esa yang sempurna yang sangat berbeda dengan makhluk ciptaan lain nya. Manusia berkembang secara dinamis, dan dalam menjalani kehidupannya manusia sangat membutuhkan manusia yang lain atau orang lain, atau manusia adalah sebagai maklhuk sosial, baik dalam berinteraksi, berkomunikasi, bergaul maupun dalam memenuhi kebutuhan-kebutuhan hidupnya.

Seiring dengan perkembangan hubungan antara manusia yang satu dengan yang lain, pastilah aakan menuimbulkan suatu sengketa atau permasalahan diantara mereka,

akan tetapi disisi lain lagi keberadaan manusia sebagai manusia yang berkembang secara dinamis akan menentukan juga perkembangan ilmu pengetahuan dan teknologi.

Di era global ini berbagai hal positif yang bisa dimanfaatkan oleh setiap bangsa terutama bidang teknologi, kemajuan teknologi juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bukan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola modernitas yang gagal mengedepankan prinsip humanitas, tetapi juga munculnya kejahatan di alam maya yang telah menjadi realitas dunia.

Memang tidak bisa diingkari oleh siapapun, bahwa teknologi itu dapat menjadi alaf perubahan di tengah masyarakat. Demikian pentingnya fungsi teknologi , hingga sepertinya masyarakat dewasa ini sangat tergantung dengan teknologi, baik untuk hal-hal positif maupun negatif. Pada perkembangannya internet juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak akan terpikirkan terjadi. Sebuah teori menyatakan bahwa *crime is product of society it self,* yang secara sederhana dapat diartikan bahwa semakin canggih tingkat intelektualitas suatu masyarakat maka akan semakin canggih dan beraneka ragam pulalah tingkat kejahatan yang dapat terjadi.[1]

Salah satu contoh terbesar saat ini adalah kejahatan maya atau biasa disebut "c*ybercrime*" (tindak pidana mayantara), merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Beberapa sebutan diberikan pada jenis kejahatan baru ini dai dalam berbagai tulisan , antara lain: sebagai "kejahatan dunia maya "(*cyberspace/virtual-space offence*), dimensi baru dari "*hi-tech crime*", dimensi baru dari "*transnational crime*", dan dimensi baru dari "*white collar crime*". [2]

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara secara global. Perkembangan teknologi informasi dan kominikasi telah pula menyebabkan perubahan dunia menjai tanpa batas (*borderless)* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara

---

[1] Abdul Wabib dan Muhammad Labib, *Kejahatan Mayantara* (*Cyber Crime*), Refika Aditama, Bandung, hal 39

[2] Barda Nawawi Arif, *Antisipasi Penanggulangan "Cyber Crime" dengan Hukum Pidana*, Makalah Pada Seminar Nasional dengan Tema "Cyber Law:, di STHB Bandung, Hotel Grand Aquila, 9 April 2001

signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum,.[3]

Saat ini telah lahir suatu rezim hukum baruyang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyberlaw* , secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaataan teknologi informasi dan komunikasi, Demikian pula hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*) dan hukum mayantara . Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem computer dan sistem komunikasi baik dalam lingkup local maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem computer yang merupakan sistem elektronik yang dapat dilihat secara virtual .[4]

Pentingnya penegakan hukum terhadap penyalahgunaan media sosial untuk menyebar kebencian dan fitnah menjadi kebutuhan utama dalam karena kejahatan ini sudah tergolong parah, jika dilihat dari perspektif hukum , sosial budaya, politik, pembangunan ekonomi, hak asasi manusia dan keamanan cbyer.[5]

Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan :[6]

1. Asas kepastian hukum, berarti landasan hukum bagi pemanfaatan teknologi informasi dan transaksi elektronik serta segala sesuatu yang mendukung penyelenggraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

---

[3] Penjelasan Undang-undang Nomor : 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[4] Penjelasan Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

[5] Renza Ardhita Dwinanda, Badrus Vian Herdik Suryanto, *Penegakan Hukum Pidana Terhadap Penyebaran Berita Bohong Di Sosial Media*, Jurnal Panorama Hukum Vol4 No:2 Desember 2019 ISSN: 2527-6654114.

[6] Pasal 3 Undang-undang Nomor : 11 Tahun 2008 Tentang Informasi dan Transkasi Elektronik beserta Penjelsannya.

2. Asas Manfaat , berarti asas bagi pemanfaatan teknologi informasi dan transaksi elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan Masyarakat.
3. Asas Kehati-hatian, berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan teknologi informasi dan transaksi elektronik.
4. Asas Itikad baik, berarti asas yang digunakan para pihak dalam melakukan transaksi elektronik tidak bertujuan untuk secara sengaja dan tanpa haka tau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengatahuan pihak lain tersebut.
5. Asas Kebebasan memilih teknologi atau netral teknologi berarti asas pemanfaataan teknologi informasi dan transaksi elektronik tidak terfokus pada penggunaan teknologi tertentu dehingga dapat mengikuti perkembangan pada masa yang akan datang.

Salah satu pertimbangan pembentukan Undang-undang Informasi dan Traksaksi Elektronik di Indonesia adalah pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfataan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.

Sementara secara umum kehadiran Undang-undang informasi dan transaksi elektronik memiliki beberapa manfaat jika dilakukan dengan benar sebagai undang-undang yang mengatur tentang informasi dan transkasi elektronik di Indonesia. Berikut ini beberapa manfaat Undang-undang Informasi dan transaksi elektronik sebagai berikut:[7]

1. Menjamin kepastian hukum untuk Masyarakat Indonesia yang melakukan transaksi elektronik;
2. Mendorong adanya pertumbuhan ekonomi di Indonesia;
3. Salah satu upaya mencegah adanya kejahatan yang dilakukan melalui internet;
4. Melindungi Masyarakat dan pengguna internet lainnya dari berbagai kejahatan orang lain.

[7] Penjelasan Undang-Undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan dengan tujuan untuk:[8]

a. mencerdaskan kehidupan bangsa sebagai bagian dari Masyarakat informasi dunia;
b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan Masyarakat;
c. meningkatkan efektivitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-;iasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi informasi seoptimal mungkin dan bertanggung jawab; dan
e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya Ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelajaan di internet. Di samping itu pembuktian merupakan factor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam system hukum acara Indonesia, secara komprehensif, melainkan juga ternayata sangat rentan untuk dibah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik, dengan demikian dampak yang diakibatkannya pun bisa demikian kompleks dan rumit[9].

Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, perkembangan teknologi informasi sekarang ini yang menimbulkan suatu kejahatan atau tindak pidana baru yaitu *cybercrime* yang bersifat transnasional walaupun sudah ada regulasi yang mengaturnya yaitu Undang-undang Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, akan tetapi perlu untuk segera

[8] Pasal 4 Undang-Undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[9] Penjelasan Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Eelektronik

dipikirkan upaya penanggulangan tindak pidana ini melalui cara penal, dimana dengan upaya atau cara penal atau dengan menggunakan hukum pidana saat ini masih terdapat keterbatasan dalam implementasinya, oleh karena itu harus diimbangi dengan cara atau upaya non-penal atau upaya diluar hukum yang bersifat preventif atau pencegahan yang harus dilakukan dalam menanggulangi tindak pidana teknologi informasi.

II. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yang berjenis Yuridis Normatif yaitu penelitian hukum yang diperoleh dari studi kepustakaan, dengan menganalisis suatu permasalahan hukum melalui peraturan perundang-undangan khususnya Undang-undang Nomor: 19 Tahun 20016 Tentang Perubahan Undang-undang Nomor;11 tahun 2008 Tentang Informasi dan Tranksaksi Elektronik., literatur dan bahan-bahan referensi laiinya yang berhubungan dengan Upaya penanggulangan tindak pidana informasi.

Pendekatan yang dipergunakan adalah pendekatan perundang-undangan (*statute approach*). Pendekatan perundang-undangan dilakukan dengan menelaah undang-undang dan regulasi yang bersangkutan langsung dengan issue hukum yang dihadapi dan Pendekatan konseptual merupakan pendekatan yang bermula dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum

Penelitian ini dilakukan dengan mengumpulkan bahan hukum melalui studi kepustakaan atau studi literature. Melalui studi kepustakaan dihimpun informasi yang relevan dengan topik atau permasalahan yang dibahas terkait dengan Upaya Penal dan Non-Penal dalam Menanggulangi tindak pidana Teknologi Informasi yang diperoleh melalui buku, jurnal, karya ilmiah, hasil penelitian, dan sumber -sumber lain.

III. PEMBAHASAN

1. Kepastian Hukum Undang-undang Informasi dan Transaksi Elektronik di Indonesia

Menurut Bab I Tentang Ketentuan Umum Pasal 1 aangka 3 Undang-undang Nomor 11 Tahun 2008 Tentang Teknologi Informasi dan Transaksi Elektronik, bahwa yang dimaksud dengan Teknologi Informasi adalah: Suatu Teknik untuk mengumpulkan, menyiapkan, meyimpan, memproses, mengumumkan, menganalisa, dan /atau menyebarkan informasi.

Permasalahan penegakan hukum di dunia virtualnya/ maya, yurisdiksi dan hukum yang berlaku terhadap suatu sengeta multi-yurisdiksi akan bertambah penting dan kompleks. Hal ini penting untuk diperhatikan mengingat seringkali disatu sisi kewenangan aparat penegak hukum dalam melakukan penegakan hukum dibatasi oleh wilayah suatu Negara yang berdaulat penuh sebagai batas dari yurisdiksi hukum yang dimilikinya, disisi lain para pelaku kejahatan dapat bergerak bebas melewati batas negara selama dilengkapi dokumen keimigrasian yang memadai,akibatnya sangat sulit bagi suatu negate untuk mengungkap sekaligus menangkap pelaku kejahatan tersebut.

Yurisdiksi adalah kekuasaan atau kompetensi hukum Negara terhadap orang, benda atau peristiwa (hukum), Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan Negara, kesamaan derajat Negara dan prinsip tidak campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah , menciptakan atau mengakhiri suatu hubungan kewajiban hukum.[10]

Undang-undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/ atau dilakukan oleh warga Negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga Negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaataan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas territorial atau universal .[11]

Terkait dengan yurisdiksi dan digunakan sarana penal satu negara (yang melakukan kriminalisiasi dengan menggunakan perundang-undangan pidana), bukan berarti dapat tertanggulangi. Karena masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana yaitu kebijakan legislasi atau formulasi atau kriminalisasi. Namun sebagaimana dikemukakan oleh Barda Nawawi Arief [12] bahwa perlu ada harmonisasi, kesepakatan dan kerja sama antar Negara mengenai yurisdiksi serta

---

[10] Shaw, *International Law*, London, Butterworths 1987, ha. 342, Sebagaimana Dikuitp Oleh Didik. M, Arif Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Infornasi*, Rafika Aditama, Bandung, 2005, hal 30

[11] Penjelasan Pasal 2 Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Eelektronik

[12] Barda Nawawi Arif, *Tindak Pidana Mayantara*, Raja Granfindo Persada, Jakarta, 2006, hal 10-11

kebijakan penal (hukum pidana) dalam penanggulangan *cybercrime* di berbagai negara.

Dalam kehidupan bermasyarakat, berbangsa dan bernegara, hak dan kebebasan melalui penggunaan dan pemanfaataan Teknologi Informasi tersebut dilakukan dengan mempertimbangkan pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatanatas hak dan kebebasaanorang lain dan untuk memenuhi tuntutnan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanaan dan ketertiban umum dalam suatu masyarakat demokratis. Undang-undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang pertama di bidang Teknologi dan Tranksaksi Elektonik sebagi produk legislasi yang sangat dibutuhkan dan telah menjadi ujung tombak yang meletakkan dasar pengaturan di bidang pemanfaataan Teknologi Informasi dan Transaksi Elektronik, walaupun dalam kenyataannya, selama pelaksanaan dari UU ITE mengalami beberapa masalah. Kesatu terhadap Undang-undang ini telah diajukan beberapa kali uji materiil di Mahkamah Konstitusi dengan Putusan Mahkamah Konstitusi Nomor: 50/PUU-VI/2008, Nomor: 2 /PUU -VII/2009, Nomor: 5/PUU-VIII/2010, dan Nomor: 20/PUU-XIV/2016 . Berdasarkan Putusan Mahkamah Konsstitusi, Nomor: 50/PUU-VI/2008, Nomor: 2 /PUU -VII/2009, tindak pidana penghinaan dan pencemaran nama baik dalam bidang Informasi Elektronik dan Transaksi Elektronik bukan semata-mata sebagai tindak pidana umum, melainkan sebagai delik aduan

Mengingat penggunaan transaksi elektrinikini terus meningkat, maka sangat diperlukan penyaring hukum untung mengaturnya untuk itulah UU ITE menjadi urgent (penting) dan mendesak untuk segara diimplementasikan. UU ITE ini diharapkan memberikan manfaat, guna menjamin kepastian hokum bagi masyarakat yang melakukan transaksi elektronik, mendorong pertumbuhan ekonomi , mencegah terjadinya kejahatan berbasis teknologi informasi dan melindungi masyarakat pengguna jasa dengan memanfaatkan ternologi informasi. Landasan hukum bagi pemanfaataan teknologi informasi dan transaksi elektronik serta segala sesuatu yang mendukung penyelenggraanya yang dapat pengakuan hukum di dalam dan di luar pengadilan .Penegasan mengenai delik aduan dimaksudkan agar selaras dengan teori kepatian hukum dan rasa keadilan masyarakat . Berdasarkan putusan Mahkamah

Konstitusi Nomor : 5/PUU-VII/2010, Mahkamah Konstitusi berpendapat bahwa kegiatan dan kewenangan penyadapan merupakan hal yang sangat sensitife karena disatu sisi merupakan pembatasan hak azasi manusia, tetapi disisi lain memiliki aspek kepentingan hukum. Oleh karena itu, pengaturan (regulation) mengenai legalitas penyadapan harus dibentuk dan diformulasikan secara tepat sesuai dengan Undang-undang Dasar Negara Republik Indonesia Tahun 1945. Disamping itu Mahkamah berpendapat bahwa karena penyadapan merupakan pelannggaran atas hak azasi manusia sebagaimana ditegaskan dalam Pasal 28 J ayat(2) Undang-undang Dasar Negara Republik Indonesia Tahun 1945 sangat wajar dan sudah sepatutnya jika Negara ingin menyimpangi hak privasi warga Negara tersebut, Negara haruslah menyimpanginya dalam bentuk undang-undang dan bukan dalam bentuk peraturan pemerintah Berdasarkan Putusan Mahkamah Konstitusi Nomor: 20/PUU-XIV/2016 Mahkamah Konstitusi , Berpendapat bahwa untuk mencegah terjadinya perbedaan penafsiran terhadap Pasal 5 ayat (1) dan ayat (2) UU ITE Mahkamah , menegaskan bahwa setiap intersepsi harus dilakukan secara sah, terlebih lagi dalam rangka penegakan hukum. Oleh karena itu , Mahkamah dalam amar putusan nya menambahkan katau atau frasa "khususnya"terhadap frasa "Informasi Elektronik" dan/ atau "Dokumen Elektronik" . bahwa ptusan tersebut akan mempersempit makna atau arti yang terdapat dalam Pasal 5 ayat (1) dan ayat (2) UU ITE agar tidak terjadi penafsiran , guna memberikan kepastian hukum keberadaan INformasi Elektronik dan/ atau Dokumen Elektronik sebagai alat bukti perlu dipertegas kembali dalam Penjelasan Pasal 5 UU ITE. [13]

Dalam pemanfataan Teknologi Informasi perlindungan , data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandungpengertian sebagai berikut:

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.

[13] Penjelasan Undang-undang Nomor : 11 Tahun 2008 Tentang Informasi dan Transaksi Eelektronik

c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang, artinya memaknai HAM dalam konteks Indonesia tidak boleh dilepaskan dari dasar falsafah yang dijadikan pedoman pelaksanaan HAM di Indeonesia.

Dasar falsafah hak asasi manusia di Indonesia adalah terletak pada adanya keseimbangan dengan kewajiban asasinya sebagai anggota masyarakat. Pemikiran ini berimplikasi bahwa dalam hak asasi manusia kepentingan pribadi seseorang tetap diletakkan dalam kerangka kesadaran kewajiban masyarakatnya, dan kewajiban terhadap masyarakat dirasakan lebih besar dari kepentingan seseorang. Dengan kata lain, disamping sadar akan kewajibannya manusia Indonesia perlu juga mengetahui hak-haknya sebagai perorangan dan anggota masyarakat . Implementasi hak asasi manusia harus senantiasa dikaitkan dengan kewajiban asasi sebagai bagian dari masyarakat.[14]

2. Tindak Pidana Teknologi Informasi di Indonesia

Cybercime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*), Menurut Sutanto,[15] secara garis besar *cybercrime* terdiri dari dua jenis , yaitu:

1. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas, Contoh-contohdari aktivitas *cybercrime* jenis pertama ini adalah pembajakan (*copyright* atau hak cipta intellektual, dan lain-lain); pornografi; pemalsuan dan pencurian kartu kredit (*carding*); penipuan lewat e-mail; penipuan dan pembobolan rekening bank; perjudiuan on-line; terorisme; situs sesat; materi-materi internet yang berkaitan dengan SARA (seperti penyebaran kebencian etnik dan rasa tau agama); transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain.
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran. *Cybercrime* jenis ini bukan memanfaatkan computer dan internet sebagai

[14] Barda Nawawi Arif, *Tindak Pidana Mayantara , Perkembangan Kajian Cyber Crime DI Indonesia*, Raja Grafindo Persada, Jakarta, 2005, hal 74
[15] Sutanto, Hermawan Sulistyo dan Tjuk Sugiatro, *Cyber Crime Motif dan Penindakan*, Pensil 324, Jakarta, hal 21

media atau sarana tindak pidana, melainkan menjadikannya sebagai sasaran. Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu system secara illegal (*hacking)*, perusakan situs internet dan server data (*cracking)*, serta *defacting*.

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan teknologi informasi dalam beberapa literature dan praktiknya menurut Mas Wigantoro dikelompokkan dalam beberapa bentuk antara lain [16]

1. *Unaouthorized Acces to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik system jaringan komputer yang dimasukinya.

2. *Illegal Contens*

   Merupakan kejahatan dengan 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*

   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

4. *Cyber Espionage*

   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system)* pihak sasaran

5. *Cyber Sabotage and Extortion*

   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. *Offence Againts Intellectual Property*

   Kejahatan ini ditujukan terhadap ha katas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs

[16] Mas Wigantoro Roes Setiyadi , *Naskah Akademik RUU Tindak Pidana Di Bidang Teknologi Informasi* , Cyber Policy Club dan Indonesia Media Law and Policy Center, 2003, hal 25

milik orang lain secara *illegal*, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainya .

7. *Infringements of Privacy*

   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain akan dapat merugikan korban secara materiil mapun immaterial, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Berdasarkan beberapa tindak pidana yang berkaitan dengan teknologi informasi di atas, Menurut RM.Roy Suryo kasus-kasus *cybercrime* yang banyak terjadidi Indonesia setidaknya ada tiga jenis berdasarkan modusnya yaitu:[17]

1. Pencurian Nomor Kredit

   Penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus cybercrime terbesar yang berkaitan dengan dunia bisnis internet di Indonesia . Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau on-line . Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di internet .

2. Memasuki, Memodifikasi, atau merusak *Homepage* (*Hacking)*

   Tindakan hacker Indonesia belum separah aksi di luar negeri Perilaku hacker Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri hacker sudah memasuki sistem perbankan dan merusak data base bank.

3. Penyerangan situs atau e-mail melalui virus atau *spamming* .

   Modus yang paling sering terjadi adalah mengirim virus melalui e-mail. Menurut RM Roy Suryo , di luar negeri kejahatan seperti ini sudah diberikan hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

[17] Majalah Warta Ekonomi, *NO:9, 5 Maret 2001, hal 12*

Dengan memperhatikan jenis-jenis kejahatan sebagaimana yang dikemukakan di atas dapat digambarkan bahwa *cybercrime* memiliki ciri-ciri khusus , yaitu: [18]

1. *Non Violence* (Tanpa kekerasan);
2. Sedikit melibatkan kontak fisik;
3. Menggunakan peralatan dan dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.

Apabila memperhatikan ciri ke-3 dan ke-4 yaitu menggunakan peralatan dan teknologi serta memanfaatkan jaringan telematika global, Nampak jelas bahwa *cybercrime* dapat dilakukan dimana saja , kapan saja,serta berdampak kemana saja, seakan-akan tanpa batas (*borderless*). Keadaan ini mengakibatkan pelaku kejahatan, korban, tempat terjadinya perbuatan pidana (*lucus delicti*) serta akibat yang ditimbulkannya dapat terjadi pada beberapa Negara. Oleh karena itu dalam memberantas kejahatan dalam dunia maya ini diperlukan penanganan yang serius serta melibatkan kerjasama internasional baik yang bersifat regional maupun multilateral.

Adapun perbuatan yang dilarang dalam Undang-undang baik Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Infromasi dan Transaksi Elektronik.

Pasal 27 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan:

1) 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 yang melanggar kesusilaan.
2) 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 perjudian.
3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik

[18] *Romli Atma Sasmita, Ruang Lingkup Berlakunya Hukum Pidana Terhadap Kejahatan Transnasional Terorganisir*, Artikel dalam Padjadjaran, Jilid XXIV NO,2 Tahun 1996, hal 90

dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Sebagai ketentuan yang mengatur kaidah larangan dan memuat sanksi pidana, maka rumusan Pasal 27 ayat (3) terikat dengan syarat *lex certa*, yakni, dengan memberikan penjelasan sera terperinci dan rumusan yang cermat atas perbuatan pidana yang diformulasikan. Dalam perkembangannya hukum pidana dalam peraturan perundang-undangan di luar KUHP telah berkembang sedemikian pesat , namun pada hakekatnya ketentuan pidana dalam undang-undang yang tersebar diluar KUHP dalam pandangan system hokum pidana tidak boleh meninggalkan asas-asas umum dan tetap mendasarkan pada ketentuan yang terdapat pada Buku I KUHP. Hal ini disadari oleh Indonesia bahwa keterbatasan perundang-undangan konvensional yang dimiliki sulit untuk untuk menjawab masalah ini, sehingga memandang perlu untuk menyesuaikan hukumnya untuk tetap menjaga untuk tetap menjaga kedaulatan Negara serta kepentingan Negara dan warganya.

Pasal 28 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan:

1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2) 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).

Pasal 29 Undang-undang Nomor: 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30 Undang-undang Nomor: 11 Tahun 2008 Tentang ITE menyatakan:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik 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, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undangundang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum 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 publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor,mendistribusikan, menyediakan, atau memiliki:
   a) perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
   b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35 Undang-undang Nomor: 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36 UU Undang-undang Nomor: 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain. Pasal 37 Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai

dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Keberadaan Informasi Elektronik dan/atau Dokumen Elektoronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastikan hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan, melalui sistem elektronik.. Ketentuan pidana yang diatur dalam Undang-undang Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-undang-undang Nomor: 11 Tahhun 2008 Tentang Informasi dan Transkasi Elektronik.

Pasal 45 menyatakan :

1) 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 yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
2) 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 perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).
3) 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 penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).
4) 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 sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan

pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Pasal 45 A:

1) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
2) Setiap Orang yang 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) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 45 B: Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Penjelasan Pasal 45 ayat (4) ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hokum yang memenuhi unsur sebagaimana dimaksud dalam pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi *(corporate crime)* dan/atau oleh pengurus dan/atau staf yang memiliki kapasatitas untuk: kapasitas untuk:

a. mewakili koorporasi;
b. mengambil keputusan dalam korporasi;
c. melakukan pengawasan dan pengendalian dalam korporasi;
d. melakukan kegiatan demi keuntungan korporasi.

3. Upaya Penal dan Non-penal dalam menanggulangi Tindak Pidana Teknologi Informasi

a. Upaya Penal

Kriminalisasi terhadap perbuatan dunia mayantara muncul ketika dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakatyang ssbelumnya belum diatur oleh hukum pidana. Hukum selalu berkembang dan semakin diperluas untuk mencakup situasi atau perubahan teknologi informasi yang terus berkembang dalam kehidupan masyarakat, perubahan hukum akan menuntut masyarakat dunia maya untuk menyesuaikan dengan hukum yang baru tersebut. Akan tetapi pada kenyatannya hukum itu sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti konkretnya adalah timbulnya berbagai kejahatan di dunia virtual yang ternyata belum bisa diatasi sepenuhnya oleh hokum.

Menurut Soedarto, dalam menghadapi masalah kriminalisasi harus diperhatikan hal-hal yang apada intinya sebagai berikut: [19]

1. Penggunaan hukum pidana harus memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata materiil dan spiritual berdasarkan Pancasila, sehubungan dengan ini maka penggunaan hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengugeran terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan perbuatan yang tidak dikehendaki yaitu perbuatan yang mendatangkan kerugian (materiil dan atau spiritual) atas warga masyarakat .
3. Penggunaan hukum pidana harus pula memperhitungkan prinsip biaya dan hasil.
4. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum yaitu jangan sampai ada kelampauan beban tugas .

Adapun Barda Nawawi Arief dengan mengutip pendapat Basisoni mengatakan bahwa keputusan untuk melakukan kriminalisasi dan deskriminalisasi harus berdasarkan pada faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam faktor, termasuk hal berikut:[20]

---

[19] Soedarto, *Hukum Dan Hukum Pidana*, Bandung, Akumni 1981, hal 44-42

[20] Muladi dan Barda Nawawi Arif, Teori-teori dan Kebijakan Hukum Pidana, Bandung, Alumni, 1992, hal 162

1. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil yang dicari atau yang ingin dicapai.
2. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari
3. Penilaian atau penaksiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber-sumber tenaga manusia.
4. Pengaruh sosial dari kriminalisasi dan deskriminalisasi yang berkenan dengan pengaruh-pengaruhnya yang sekunder.

Barda Nawawi Arief menjelaskan maksud dari penanggulangan tindak pidana. Penanggulangan adalah usaha yang dilakukan oleh individu seseorang ataupun lembaga dengan tujuannya memberikan keamanan dan kesejehteraan kehidupan bermasyarakat yang sesuai dengan hak asasi manusia. Tindak pidana atau kejahatan merupakan pelanggaran norma hukum yang selalu dihadapi oleh setiap masyarakat. Munculnya kejahatan tentu sangat meresahkan, kejahatan juga mengganggu ketentraman dan kenyamanan dalam masyarakat. Berbagai program dan kegiatan telah dilakukan oleh pemerintah dan dibantu masyarakat terus menerus, sampai menemukan cara efektif untuk menanggulangi masalah kejahatan ini.[21]

Upaya penanggulangan kejahatan secara garis besar dapat dibagi 2 (dua) , yaitu lewat jalur "*penal*" (hukum pidana) dan lewat jalur "*non-penal* " (bukan/di luar hukum piada). Penerapan hukum pidana (*criminal law application*) tidak terlepast dari adanya peraturan perundang-undangan pidana, menurut Soedarto, usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang berarti melaksanakan politik hukum pidana [22]

Politik hukum pidana dalam kepustakaan asing sering dikenal dengan "*penal policy*". *Penal policy* menurut Marc Ancel,[23] adalah upaya menanggulangi kejahatan dengan pemberian sanksi pidana atau penal. Sebagai "suatu ilmu

[21] Ibid.hal.6
[22] Soedarto.Op-cit hal.78
[23] Ibid

sekaligus seni yang bertujuan untuk memungkinkan peraturan positif dirumuskan secara lebih baik".

Kebijakan hukum dengan sarana "*penal*" (pidana) merupakan serangkaian proses yang terdiri atas tiga tahap yakni: [24]

a. Tahap kebiajakan *legislative / formulatif;*
b. Tahap kebijakan *yudikatif/aplikatif;*
c. Tahap kebijakan *eksekutif/adminstratif.*

Tahapan formulasi dalam proses penanggulangan kejahatan memberikan tanggung jawab kepada aparat pembuat hukum (aparat legislative) menetapkan atau merumuskan perbuatan apa yang dapat dipidana disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatife) yang harmonis dan terpadu.

Kebijakan penal merupakan bagian dari kebijakan atau politik hukum pidana, dengan menggunakan sarana penal juga menentukan masalah perbuatan apa yang seharusnya dijadikan tindak pidana dan sanksi apa yang akan diberikan. Karena dengan adanya ancaman dan penjatuhan pidana terhadap kejahatan diharapkan adanya efek pencegahan. Hal ini berarti bahwa, hukum pidana difungsikan sebagai sarana pengendali sosial, yaitu dengan sanksinya yang berupa pidana untuk dijadikan sarana menanggulangi kejahatan. Digunakannya hukum pidana sebagai sarana menanggulangi kejahatan merupakan sesuatu yang lazim digunakan di berbagai Negara termasuk Indonesia. Hal ini terlihat dari praktik perundang-undangan yang menunjukkan bahwa penggunaan hokum pidana merupakan bagian dari kebijakan atau politik hukum pidana yang dianut oleh Indonesia.

Adapun kebijakan criminal menurut Barda Nawawi Arief yang dikutip dari Marc Ancel adalah pengaturan atau menyusun secara raisonal usaha-usaha pengendalian kejahatan oleh masyarakat .[25] . Diatas telah dijelaskan bahwa usaha-suaha yang rasional untuk mengendalian kejahatan atau mengurangi kejahatan (politik kriminal) ini dapat ditempuh dengan menggunakan sarana penal (hukum pidana), tetapi dapat juga dengan menggunakan sarana non-penal.

---

[24] Barda Nawawi Arif, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan……hal 78-79
[25] Barda Nawawi Arif, Bunga Rampai Kebijakan Hukum Pidana..hal 42

Menurut Barda Nawawi Arief bahwa upaya menanggulangi kejahatan melalui jalur penal lebih menitik beratkan pada sifat *repressive* (penindakan/pemeberantasan/penumpasan) sesudah kejahatan terjadi, sedangkan jalur non-penal labih menitikberatkan sifat *preventive* (pencegahan/penangkalan/pengendalian) sebelum kejahatan terjadi.[26]

Penanggulangan kejahatan dengan sarana hokum pidana berarti berate mengadakan pemilihan untuk mncapai hasil perundangan pidana yang baik dalam arti memenuhi syarat keadilan dan saya guna.[27]

b. Upaya Non-Penal

Diatas telah dijelaskan bahwa penanggulangan kejahatan melalui jalur non penal lebih bersifat tindakan pencegahan sebelum kejahatan terjadi , sehingga sasaran utamaya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan .

Menurut Barda Nawawi Arief, beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, , jelas merupakan masalah yang tidak dapat diatasi semata-mata dengan jalur "*penal*". Disinilah keterbatasan jalur "*penal*" dan oelah karena itu harus ditunjang oleh jalur *"non-penal*".

Kebijakan kriminal menggunakan sarana non-penal menitikberatkan menitik beratkan pada sifat preventif (pencegahan/penangkalan/pengendalian)sebelum kejahatan terjadi . Mengingat upaya penanggulangan kejahatan lewat jalur non-penal lebih bersifat tindakan pencegahan untuk terjadinya kejahatan, maka sasaran utamanya adalah menangani faktor-faktor kondusfifpenyebab terjadinya kejahatan. Faktor-faktor kondusif itu antara lain berpusat pada masalah –masalah atau kondisi-kondisi sosialyang secara langsung atau tidak langsung dapat menimbulkan atau menumbuh suburkan kejahatan . Dengan demikian, dilihat dari sudut politik kriminal secara makro dan global, maka upaya non-penal menduduki posisi kunci dan strategis dari keseluruhan upaya politik kriminal. Beberapa masalah dan kondisi sosialyang dapat menjadi faktor kondusif timbulnya kejahatan tidak dapat diatasi semata-mata dengan upaya penal, karena keterbatasan upaya karena keterbatasan

[26] Ibid , hlm 2
[27] Ibid, hlm 6

upaya penal, disinilah harus ditunjng dengan adanya upaya non-penal untuk mengatasi masalah-masalah sosial maupun masalah kesehatan jiwa masyarakat yang dapat menimbulkan kejahatan. Penanggulangan kejahatan dengan sarana non-penal berupa pencegahan tanpa pidana dan mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan melalui media massa.[28]

Mengingat upaya penanggulangan kejahatan lewat jalur non- penal lebih bersifat tindakan pencegahan untuk terjadinya kejahatan, maka sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan . Faktor-faktor kondusif ini antara lain antara lain berpusat pada masalah-masalah atau kondisi-konsisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhsuburkan kejahatan. Dengan demikian secara makro dan global, maka upaya –upaya non-penal menduduki posisi kunci dan strategis dalam menanggulangi sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan.[29]

Usaha-usaha non-penal ini misalnya dengan pendidikan dalam rangka mengembangkan tanggung jawab sosial warga masyarakat , penggarapan tanggung jawab sosial warga masyarakat, penggarapan kesehatan jiwa masyarakat melalui pendidikan moral, agama dan sebagainya.

Penanggulangan kejahatan menggunakan upaya non-penal perlu digali, dikembangkan dan memanfaatkan seluruh potensi dukungan dan partisipasi masyarakat dalam upaya untuk mengefektifkkan dan mengembangkan "*extra legal system atau informal and traditional system*" yang ada dalam masyarakat . Selain itu upaya non-penal juga dapat ditempuh dengan menyehatkan lewat kebijakan sosial dan dengan menggali berbagai potensi yang ada di dalam masyarakat itu sendiri, dapat pula upaya non-penal itu digali dari berbagai sumber lainnya yang juga mempunyai potensi efek preventif. Sumber lain misalnya media pers, media masaa, pemanfaataan teknologi dan pemanfaatan potensi efek preventif dari dari aparat penegak hokum. Mengenai potensi efek preventif aparat penegak hukum . ini dilakukan menurut Soedarto, bahwa kegiatan patrol dari polisi yang dilakukan

[28] Barda Nawawi Arif, Kebijakan Legislatif dalam Menanggulangi Kejahatan Dengan Pidana Penjara, Bandung , Alumni, 1994, hal 13

[29] Ibid, hlm 3 9

secara kontiyu upaya non-penal yang mempunyai pengaruh preventif bagi penjahat (pelanggar hukum)[30]

Berdasarkan beberapa pendapat diats mengenai upaya penanggulangan kejahatan secara non-penal dalam kebijakan penanggulangan kejahatan , cukup beralasan kiranya untuk terus menerus menggali, memanfaatkan dan mengembangkan upaya-upaya non-penal untuk mengimbangi kekurangan dan keterbatasan sarana penal .

Kebijakan penanggulangan kejahatan dengan sarana non-penal hanya meliputi penggunaan sarana sosial untuk memperbaiki kondisi-kondisi sosial tertentu, namun secara tidak langsung mempengaruhi upaya terjadinya kejahatan.

Penagakan dan politik criminal dalam penanggulangan kejahatan atau tindak pidana, sebagai upaya membuat hukum berfungsi, beroperasi atau bekerja serta terwujud secara konkret. Bertolak dari pengertian yang demikian maka fungsionalisasi atau proses penegakan hukum umumny melibatkan melibatkan minimal tiga faktor yang saling berkaitan/terkait. Adapun tiga faktor tersebut yaitu faktor perundang-undangan, faktor ini dapat dikaitkan dengan pembagian tiga komponen sistem hukum yaitu aspek substansi (*legal substantion*), aspek struktural(*legal stucture)*, aspek budaya hukum (l*egal culture*), maka suatu kebijakan hukum dapat dipengaruhi oleh faktor tersebut.[31]

IV. KESIMPULAN

Upaya Penal dalam menanggulangi tindak pidana teknologi informasi yang dilakukan secara penal adalah bersifat *repressive* atau melakukan penindakan, penumpasan, pemberantasan setelah tindak pidana terjadi, sudah diamanatkan dalam Undang-undang Nomor 11 Tahun 2008 Tentang Teknologi Informasi dan Transaksi Elektronik dan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Teknologi Informasi dan Transaksi Elektronik, walaupun dalam kebijakan aplikatifnya atau implemantasinya masih terdapat keterbatasan diantaranya adalah sebagai berikut:

[30] Ibid hal.50
[31] Ibid.55

a. Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrim*e. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), dan kejahatan yang ditimbulkannya, karena di dalam melakukan penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi dari aparat penegak hukum dan belum semua negara memilikinya mengingat perbuatan kejahatan yang dilakukan berada di lingkungan elektronik.
b. *Cybercrime* melampaui batas-batas negara, atau antar lintas negara atau bersifat transnasional sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah teritorial negaranya sendiri.
c. Struktur terbuka dari jaringan komputer internasional memberikan peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *cybercrime*. Terjadinya data havens (negara tempat berlindung atau singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghambat usaha negara lain untuk memberantas kejahatan itu.
d. Lebih ditingkatkan tentang harmonisasi, kesepakatan, dan kerjasama antar negara mengenai yurisdiksi serta kebijakan penal (hukum pidana) dalam penanggulangan *cybercrime* diberbagai negara.

Upaya Non-Penal dalam menanggulangi tindak pidana teknologi informasi yang, adalah bersifat *preventif* atau pencegahan , penangkalan, pengendalian sebelum tindak pidana terjadi, sebaiknya dilakukan dengan kemampuan dan kemauan yang didasarkan kepada hal-hal sebagai berikut:

a. Diperlukan kerjasama internasional untuk menelusuri/mencari para penjahat di internet;
b. Perlu ada harmonisasi, kesepakatan, dan kerjasama antar negara mengenai yurisdiksi serta kebijakan Non- penal (di luar hukum pidana) yang disesuaikan dengan kondisi masing-masing negara dalam penanggulangan c*ybercrime* diberbagai Negara;
c. Harus ada penegasan untuk melakukan kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar

internet menjadi tempat yang aman dalam pemanfaatan perkembangan teknologi di era teknologi informasi;

d. Melakukan edukasi pendidikan kepada masyarakat tentang pemahaman penggunaan komputer terhadap keamanan *Cyber*, misalnya dengan ditingkatkannya berita-berita yang mengedukasi masyarakat melalui Media Masaa maupun Media Elektronik, disamping juga melakukan penyuluhan dan sosialisasi yang dilakukan oleh pihak yang berwenang.

DAFTAR PUSTAKA

Buku-Buku

Abdul Wahib dan Muhammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime),* Refika Aditama, Bandung.

Barda Nawawi Arif, 1994, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Ananta, Semarang.

----------. 1994, *Bunga Rampai Kebijakan Hukum Pidana*, Raja Grafindo Persada, Jakarta.

----------,2005, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime Di Indonesoa*, Raja Grafindo Persada, Jakarta.

---------- 2006, *Tindak Pidana Mayantara*, Raja Granfindo Persada, Jakarta,

----------, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Kencana Predana Media Grup, Jakarta.

Dikdik M.Arif Mansur dan Elisatris Gultom, 2005, *Cyber Law: Aspek Hukum Teknologi Informas*i, Refika Aditama, Bandung.

Moeladi dan Barda Nawawi Arif, 1998, *Teori-teori dan Kebijakan Pidana*, Alumni, Bandung,

Soedarto, 1981, *Hukum dan Hukum Pidana*, Alumni, Bandung.

Sutanto Hermawan Sulisyto dan Tjuk Sugiarto, 2002, *Cyber Crime Motif dan Penindakan*, Pensil 324, Jakarta.

Peter Mahmud Marzuki, 2005, *Peneltian Hukum*, Prenada Media , Jakarta.

Peraturan Perundang-undangan

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang *Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaski Elektronik*.

Undang-undang Nomor 11 Tahun 2008 Tentang *Informasi dan Transaski Elektronik*.

Putusan-Putusan

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010.

Putusan Mahkamah Konstitusi Nomor 2/PUU-VII/2009.

Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008.

Artikel dalam Jurnal

Romli Atma Sasmita, *Ruang Lingkup Berlakunya Hukum Pidana Terhadap Kejahatan Transnasional Terorganisir*, Artikel Dalam Padjadjaran, Jilis XXIV No.22 Tahun 1996.

Renza Ardhita Dwinanda, Badrus Vian Herdik Suryanto, *Penegakan Hukum Pidana Terhadap Penyebaran Berita Bohong Di Sosial Media,* Jurnal Panorama Hukum Vol.4 No. 2 Desember 2019, ISSN: 2527-6654114.

Majalah Warta Ekonomi, *No.9, 5 Maret 2001.*