KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA PENANGANAN CYBER CRIME YANG DILAKUKAN OLEH *VIRTUAL POLICE* DI INDONESIA

Utin Indah Permata Sari
Fakultas Hukum, Universitas Brawijaya
E-mail : indahhpermata05@gmail.com

ABSTRACT

Tujuan dilakukannya penelitian ini adalah untuk memahami kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini dalam menangani cyber crime, menganalisa dan menggambarkan kebijakan regulasi hukum pidana terhadap tindak pidana teknologi dalam menangani kasus cyber crime di masa yang akan datang, mengetahui dan meneliti apa saja kasus cyber crime yang pernah terjadi di Indonesia yang memiliki dan yang tidak memiliki ketentuan hukumnya, serta dapat mengetahui efektivitas peran virtual police dalam menangani tindakan masyarakat yang berpotensi melanggar Undang-undang Informasi dan Transaksi Elektronik. Metode penelitian yang digunakan dalam penelitian ini adalah hukum normatif karena fokus kajian berdasarkan pada doktrin melalui analisis kaidah hukum yang ditemukan dalam peraturan perundang-undangan atau dalam berbagai putusan pengadilan dengan menggunakan bahan penelitian yang bersifat primer, sekunder, dan tersier. Hasil penelitian yang dapat dijadikan sebagai kesimpulan dalam penelitian ini adalah penegakan hukum dalam penanggulangan cyber crime di Indonesia belum dilaksanakan secara optimal. Faktor-faktor yang akan mempengaruhi penegakan hukum terhadap cyber crimes meliputi faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas dalam penegakan hukum, dan faktor masyarakat. Kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia cyber yang semakin canggih. Pentingnya kesadaran masyarakat untuk mencapai tujuan selain upaya dari kepolisian dalam menanggulangi cyber crime.

Kata Kunci : polisi virtual, hukum pidana, kejahatan siber.

ABSTRACT

The purpose of this research is to understand the policy of criminal law regulation against information technology crimes at this time in dealing with cyber crime, analyze and describe the policy of criminal law regulations against technological crimes in dealing with cyber crime cases in the future, find out and research anything cyber crime cases that have occurred in Indonesia that have and do not have legal provisions, and can find out the effectiveness or the virtual police role in dealing with public actions that have the potential to violate the Law on Information and Electronic Transaction. The research method used in this study is normative law because the focus of the study is based on doctrine through analysis of legal rules found in law and regulations or in various court decisions using primary, secondary, and tertiary research materials. The result of this research that can be used as a conclusion in this research is that law enforcement in overcaming cyber crime in Indonesia has not been implemented optimally. Factors that will affect law facilities in law enforcement and community factors. The policy of criminalizing acts in cyberspace must continue to be harmonized with the rise of crime in the increasingly sophisticated cyber world. The importance of public awareness to achieve goals othe than efforts of the police in tackling cyber crime.

***Keyword** : virtual police, criminal law, cyber crime.*

A.PENDAHULUAN

Dewasa ini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi dalam berbagai aspek kehidupan manusia. Perkembangan teknologi informasi dan komunikasi menyebabkan adanya media baru berupa internet yang menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan. Kehidupa manusiadi zaman sekarang ini sangat bergantung pada teknologi. Di satu sisi,teknologi dapat membawa banyak dampak positif, seperti adanya E-mail, E-commerce, Cyber bank, Online Business, Internet Banking, dan sebagainya. Namun, di sisi lain juga membawa dampak negatif dengan munculnya cyber crime.
Dinamika kemajuan teknologi informasi dan komunikasi dalam masyarakat saat ini selain memberikan dampak positif, juga memberikan dampak negatif dari akibat ketidaksesuaian penggunaannya yang mengakibatkan timbulnya suatu kejahatan yang dikenal dengan istilah kejahatan siber (Arief, 2012).

Pengertian dari kejahatan dunia maya atau cyber crime merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi dengan menggunakan internet sebagai media untuk melakukan tindak kejahatan.

Kemajuan teknologi berimplikasi pada perkembangan kejahatan. Kejahatan yang dulunya dianggap sebagai suatu kejahatan apabila adanya kontak fisik antara pelaku dan korban dalam melakukan tindak kejahatan bertransformasi menjadi kejahatan di dunia maya atau cyber crime yang dapat dilakukan tanpa adanya kontak fisik antara pelaku dan korban secara langsung dengan menggunakan media internet dan alat elektronik lainnya. Dampak dari adanya internet memberikan peluang kepada para pelaku kejahatan untuk melakukan kejahatan yang lebih tersembunyi dapat menembus ruang dan waktu dengan jangkauan yang luas, bahkan global.

Kejahatan di dunia maya dapat dilakukan dimana dan kapan saja dengan syarat adanya jaringan internet dan peralatan yang memadai. Mengenai karakteristik cyber crime, Mamoun Alazab, Roderic Broadhurst Peter Grabosky, dan Steve Chon mengatakan "Cyber criminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national".

Berkembangnya cyber crime dapat terlihat dari munculnya berbagai istilah seperti online business crime, cyber money laundering, high tech white collar crime, dan sebagainya. Bahkan, dalam dokumen PBB, cyber crime memiliki istilah baru yaitu, Dogpiling, Dixing, Doxware, Kejahatan terkait identitas, Pelecehan seksual berbasis gambar, online impersonation, Roasting, Pharming, Sextortion, dan Zero day.
Dalam FBI Cybercrime Report 2017, Kepolisian Amerika Serikat merilis 20 negara tertinggi yang menjadi korban dari tindak kejahatan cyber crime selain Amerika Serikat diantaranya Kanada, India, Inggris, Brazil, Jerman, Australia, Spanyol, Mexico, dan beberapa negara lainnya. Indonesia tidak termasuk dalam 20 negara tertinggi yang menjadi korban cyber crime, tetapi termasuk dalam negara yang menjadi asal dimana cyber crime dilakukan.
Kasus cyber crime pertama kali di Indonesia terjadi pada tahun 1990-an dengan munculnya kasus pemakaian nama domain www.mustikaratu.com yang disidangkan di pengadilan Negeri Jakarta Selatan. Kasus ini menyeret seorang terdakwa yang bernama Tjandra Sugiono dengan dakwaan Pasal 382 bis KUHP dan Pasal 48 ayat (1) jo Pasal 19 huruf b UU Nomor 5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Dalam pemeriksaan perkara tersebut majelis hakim Pengadilan Negeri Jakarta Selatan memutuskan bahwa perbuatan yang didakwakan tidak terbukti sehingga terdakwa dibebaskan dari segala dakwaan.1

Lona Olivia melaporkan "Indonesia has received greater security from cybercrime authorities in recent years, especially since a 2013 survey by Akamai Technologies, and IT security firm, reported that Indonesia had overtaken China as the number one source of hacking traffic in the

world". Indonesia telah mendapat pengawasan yang lebih besar dari pihak otoritas cybercrime beberapa tahun terakhir, terutama sejak survei tahun 2013 oleh Akamai Technologies, sebuah perusahaan keamanan TI yang melaporkan bahwa Indonesia telah berhasil mengalahkan China sebagai sumber hacking traffic terbesar di dunia.

Dalam data statistik laporan cyber crime yang terjadi di Indonesia pada tahun 2019 terdapat 4.586 total laporan dalam kurun waktu 1 tahun, sedangkan pada tahun 2020 turun menjadi 2.259 laporan. Dalam laporan tersebut kasus penyebaran konten provokatif menduduki puncak daftar kasus tertinggi, lalu diikuti oleh kasus penipuan oline, pornografi, akses ilegal, dan kasus lainnya.

Penanganan cyber crime bukanlah suatu hal yang mudah untuk diatasi, selain karakteristik cyber crime itu sendiri, regulasi hukum di Indonesia yang sudah ada belum dapat menjangkau perkembangan kejahatan yang dilakukan di dunia maya. Peraturan Perlindungan data pribadi yang ada di Indonesia hanya didasarkan pada Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Substansi yang tercantum dalam Undang-undang Informasi dan Transaksi Elektronik atau UU ITE berisi perlindungan hak pribadi, asas perdagangan secara e- commerce, masalah yurisdiksi, asas persaingan usaha-usaha tidak sehat dan perlindungan konsumen, asas hak atas kekayaan intelektual, asas cyber crime, dan hukum internasional

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum. Politik hukum pidana merupakan bagian dari kebijakan penegakan hukum (law enforcement policy). Penggunaan upaya hukum termasuk hukum pidana, sebagai salah satu upaya mengatasi masalah sosial, termasuk dalam bidang kebijaksanaan penegakan hukum. Di samping bertujuan untuk mencapai kesejahteraan masyarakat pada umumnya, maka kebijaksanaan penegakan hukum ini pun termasuk dalam kebijaksanaan sosial, yaitu segala usaha yang rasional untuk mencapai kesejahteraan masyarakat (Arief, 2014).

Kejahatan baru ini sangat berdampak pada berbagai aspek bidang kehidupan. Banyak yang menganggap bahwa keberadaan KUHP tidak mampu menjangkau kejahatan baru tersebut sehingga pemerintah menginisiasi lahirnya aturan tentang cyber crime. Berdasarkan dokumen yang ada, Undang- undang tentang Informasi dan Transaksi Elektronik (UU ITE), yaitu Undang-undang Nomor 19 Tahun 2016 atas perubahan atas Undang-undang Nomor 11 Tahun 2008 (Hermawan, 2019).

Kesesuaian antara karakteristik pelaku cyber crime dengan paradigma pemidanaan dalam pidana kerja sosial atau pidana pengawasan sehingga tujuan pemidanaan akan dapat tercapai. Sejalan dengan pandangan Widodo, dalam mengantisipasi cyber crime, Rancangan Undang-Undang Kitab Hukum Pidana mencoba memperluas cakupan untuk dapat menjaring kejahatan cyber crime.

Menurut Widodo, penjatuhan pidana kepada para pelaku cyber crime adalah langkah yang kurang tepat dan kurang bijak. Hal ini disebabkan oleh ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistem pembinaan narapidana di Lembaga Permasyarakatan sehingga tujuan pemidanaan sebagaimana diatur dalam Undang-undang Permasyarakatan tidak akan tercapai. Menurutnya, sebagai pengganti pemidanaan tersebut adalah pidana kerja sosial atau pidana pengawasan (Widodo, 2013), sedangkan menurut Barda Nawawi Arief, jika dilihat dari sudut pandang hukum pidana, upaya penanggulangan cyber crime khususnya di Indonesia dapat dilihat dari berbagai aspek, yaitu aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), aspek kriminalisasi (formulasi tindak pidana), dan aspek yurisdiksi.

Barda Nawawi Arief mengatakan kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang

semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal (criminal policy) dengan menggunakan sarana hukum pidana (penal). Oleh karena itu, hal tersebut termasuk bagian dari 'kejahatan hukum pidana' (penal policy), khususnya kebijakan formulasinya. Selanjutnya menurut Arief, kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/ merumuskan/ memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah

Bagaimana kebijakan formulasi/legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu. Kebijakan penanggulangan cyber crime secara teknologi, diungkapkan juga dalan IIIC (International Information Industry Congress) yang menyatakan: "The IIIC recognizes that government action and international traties to harmonizes laws and coordinate legal procedurs are key in the fight against cybercrime, but warns that these should not be relied upon as the onlu instuments. Cybercrime is enabled by technology and requires a healthy reliance on technology for ots solutions".3

Sementara dalam hal menangani dan menyelidiki cyber crime adalah peran dari cyber police dan virtual police. Peran dari virtual police sendiri adalah memberikan edukasi kepada masyarakat terkait dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE), sedangkan peran dari cyber police adalah menindaklanjuti kasus jika tindakan yang dilakukan oleh masyarakat tersebut tidak bisa ditegur oleh virtual police. Singkatnya, virtual police muncul sebelum diselidiki lebih lanjut oleh cyber police.

Kepala Divisi Humas Polri Irjen Pol Raden Prabowo Argo Yuwono mengatakan cara kerja dari polisi virtual adalah dengan memberikan peringatan kepada akun di media sosial yang diduga melanggar, hal ini tentu saja dilakukan setelah adanya pertimbangan dari pendapat ahli bukan semata-mata pendapat subjektif penyidik. Selanjutnya saat akun mengunggah tulisan gambar yang berpotensi melanggar maka, petugas akan menyimpan tampilan unggahan tersebut untuk dikonsultasikan dengan tim ahli yang terdiri dari ahli pidana, ahli bahasa, dan ahli informasi dan transaki elektronik. Jika ahli mengatakan konten tersebut memuat pelanggaran pidana, langkah selanjutnya adalah diajukan ke direktur siber atau pejabat yang ditunjuk siber memberikan pengesahan. Kemudian, virtual police alert dikirim secara pribadi ke akun yang bersangkutan secara resmi. Peringatan akan dikirimkan lewat direct message, sebab kepolisian tidak ingin peringatan dari virtual police kepada pengguna media sosial tersebut diketahui oleh pihak lain, karena bersifat rahasia.

Kehadiran virtual police ini cenderung masih baru di kalangan masyarakat, padahal diketahui pihak kepolisian sudah memiliki tim siber yang fungsinya tidak jauh berbeda dengan polisi virtual. Masih banyak masyarakat yang belum mengetahui perbedaan antara polisi virtual dan polisi siber, salah satu alasannya yaitu kurangkan pengedukasian kepada masyarakat dengan cakupan yang lebih luas. Sejalan dengan hal ini, Koordinator Wilayah Peradi Jawa Tengah, Badrus Zaman menjelaskan perbedaan dari keduanya yaitu jika polisi virtual lebih mengedepankan upaya preventif, sedangkan polisi siber sudah pasti melakukan penegakan hukum sesuai regulasi yang ada karena polisi siber sudah dapat mendeteksi melanggar rambu-rambu UU ITE.

Berdasarkan uraian yang dijabarkan diatas maka permasalahan yang berkaitan dengan kebijakan penegakan hukum dalam upaya penanganan cyber crime yang dilakukan oleh virtual police di Indonesia yaitu:

1.Bagaimana kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini dalam menangani cyber crime?

2.Bagaimana sebaiknya kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi dalam menangani cyber crime yang akan datang?

3.Apa saja kasus cyber crime yang pernah terjadi di Indonesia yang memiliki maupun yang tidak memiliki pengaturan hukum?
4.Bagaimana efektivitas peran virtual police dalam menangani tindakan masyarakat yang berpotensi melanggar UU ITE?
Bertitik tolak pada permasalahan- permasalahan di atas, penelitian ini bertujuan untuk:
1.Memahami kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini dalam menangani cyber crime. (Barda Nawawi Arief, 2000)
2.Menganalisa dan menggambarkan kebijakan regulasi hukum pidana terhadap tindak pidana teknologi dalam menangani kasus cyber crime di masa yang akan datang
3.Mengetahui dan meneliti apa saja kasus cyber crime yang terjadi di Indonesia yang memiliki dan yang tidak memiliki ketentuan hukumnya
4.Mengetahui keefektifan peran virtual police dalam menangani tindakan masyarakat yang berpotensi melanggar UU ITE

Beberapa penelitian sebelumnya ada yang membahas peran kepolisian dalam menangani kasus cyber crime seperti dalam artikel yang ditulis oleh Abdul Agis yang berjudul "Peran Kepolisian dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronik". Selain itu, penelitian lainnya yang menganalisa tentang kesiapan dari aparatur yang ditulis oleh Rudi Hermawan yang berjudul "Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia". Terdapat juga penelitian yang mengusut tentang apa saja fungsi kepolisian dalam artikel yang ditulis oleh Sukinta yang berjudul "Peran Kepolisian Dalam Melakukan Penyidikan Tindak Pidana Penyebaran Berita Bohong di Indonesia". Selain dari sisi kepolisian, juga terdapat dari sudut pandang hukum yang dibahas pada artikel "Tinjauan Yuridis Efektivitas UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik" yang ditulis oleh Refland, Hero Soepono, dan Grace. Berkaitan dengan artikel tersebut, terdapat sebuah penelitian yang ditulis oleh Philemon Ginting yang berjudul "Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana". Terakhir, terdapat sebuah penelitian tentang penanggulangan cyber terorism yang ditulis oleh Dwila Annisa dan Mujiono Hafidh yang berjudul "Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism".

B.METODE PENELITIAN

Tulisan ini menggunakan metode penelitian hukum normatif karena fokus kajian berdasarkan pada doktrin melalui analisis kaidah hukum yang ditemukan dalam 4 Aloysius Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer, Universitas peraturan perundang-undangan atau dalam berbagai putusan pengadilan dengan menggunakan tiga pendekatan, yaitu pendekatan undang-undang, pendekatan konseptual, dan pendekatan kasus.

Sementara teknik pengumpulan data melalui data sekunder, yaitu dilakukan dengan cara studi dokumen dengan bahan penelitian yang bersifat primer, sekunder, dan tersier. Hasil penelitian dianalisis dan diuraikan secara deskriptif kualitatif, artinya data yang dikumpulkan dengan membandingkan antara teori yang berlaku dengan fakta-fakta yang terdapat di lapangan.

Penulisan kutipan menggunakan footnote. Susunan footnote secara berurutan adalah nama penulis, judul (cetak tebal, cetak tebal dan miring bila menggunakan bahasa asing), penerbit, tempat penerbitan, tahun penerbitan dan halaman. Untuk penulis orang Indonesia, nama pertama disebut terlebih dahulu, sedangkan untuk penulis asing nama kelurga disebut lebih dahulu, kesemuanya tanpa mencantumkan gelar. Penulisan dilakukan dengan ketentuan spasi 1 (satu) dan dimulai dengan awal footnote yang menjorok masuk sebanyak 6 karakter. Penulisan antar footnote tidak menggunakan spasi.

C.PEMBAHASAN

1.Kebijakan Hukum Pidana Terhadap Tindak Pidana Teknologi Informasi Berdasarkan Hukum Positif Saat ini Definisi kata kebjakan berasal dari

bahasa inggris yaitu pilcy atau dalam bahasa belanda disebut politiek yang dimana secara umum dapat diistilahkan sebagai dasar-dasar umum yang berfungsi untuk mengarahlan pemerintah, dalam pengertian luas termasuk pula didalamnya unsur aparat penegak hukum dalam hal mengelola, mengatur, atau menyelesaikan kepentingan-kepentingan umum, persoalan-persoalan masyarakat atau permasalahan penyusunan peraturan perundang-undangan dan pengaplikasikan hukum atau peraturan dengan tujuan umum yang menjurus kepada upaya mewujudkan kesejahteraan ataupun keadilan dalam masyarakat. (Atmajaya Yogyakarta, Yogyakatya, 1999, Hal. 10)

Digunakan hukum pidana di Indonesia sebagai suatu sarana untuk menanggulangi suatu bentuk kejahatan sepertinya tidak menjadi permasalahan yang mendasar, hal ini dapat dilihat dari adanya praktik perundang-undangan yang selama ini menunjukkan bahwa penggunaan hukum pidana merupakan bentuk bagian yang tak terpisahkan dari kebijakan atau politik hukum yang digunakan oleh Indonesia. Penggunaan hukum pidana selama ini dianggap sebagai hal yang normal, artinya dengan kondisi tersebut eksistensinya sudah tak lagi dipermasalahkan. A

Dalam Kitab Undang-Undang Hukum Pidana Kitab Undang–Undang Hukum Pidana yang biasa disingkat menjadi KUHP merupakan sistem utama bagi peraturan-peraturan hukum pidana di Indonesia. Perumusan tindak pidana yang tercantum dalam KUHP mayoritas masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan dari cyber crime itu sendiri. Beberapa peraturan perundang- undangan yang berhubungan dengan tindak pidana teknologi informasi diluar dari pengaturan KUHP yaitu:

1)Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

2)Undang-Undang Nomor 19 Tahun 2002 Tentang Hak Cipta

3)Undang-Undang Nomor 25 Tahun 2003 Tentang Perubahan atas Undang- Undang Nomor 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang

4)Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

b.Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Seiring dengan perkembangan zaman, dan dalam mengatur cyber space dan cyber crime telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi.

Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di cyber space.

Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan " Setiap orang berhak untuk mencari, memperoleh, memiliki, meyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia".

Tindakan-tindakan cyber crime yang dimuat dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu, sebagai berikut :

1)Tindakan yang melanggar kesusilaan Dalam Pasal 27 ayat (1) UU Nomor

11 Tahun 2008 disebutkan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan danatau

mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan", tetapi dalam pasal tersebut tidak dijelaskan mengenai perbuatan yang (Mudadi & Barda Nawawi, Teori-teori dan Kebijakan Pidana, PT. Alumni Bandung, 2010, Hal. 157). memiliki muatan yang melanggar kesusilaan.

Sementara dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, terdapat beberapa tindakan yang tergolong dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008, yaitu cyber pornografi dan prostitusi online. Tindak pidana ini akan semakin berat hukumannya apabila dilakukan terhadap anak di bawah umur. Salah satu permasalahan yang ditimbulkan dari kemajuan teknologi informasi melalui jaringan internet adalah beragamnya situs yang menampilkan adegan pornografi. Seolah-oleh sekarang ini, sulit sekali memproteksi jaringan internet dari serbuan pebisnis hiburan yang menjual pornografi. 2)Penghinaan/Pencemaran nama baik Penghinaan/Pencemaran nama baik di cyber space diatur dalam Pasal 27 ayat (3) UU Nomor 11 Tahun 2008 yang menyatakan "Setiap orang dengan sengaja dam tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diakseskan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Dalam UU ITE ini, pembuat undang-undang menyetarakan antara penghinaan dengan pencemaran, pada penghinaan sendiri merupakan suatu kelompok perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran.

Tindakan dari penghinaan dan/atau pencemaran dapat ditemukan dalam berbagai kolom komentar di cyber space. Pelaku dapat menuliskan kata-kata yang mengandung penghinaan dan/atau pencemaran pada dinding akun korban, baik dengan atau menautkan pernyataan tersebut kepada korban.

3)Perjudian

Perjudian online diatur dalam Pasal 27 ayat (2) UU Nomor 11 Tahun 2008 yang menyatakan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau (Abdul Wahid & Mohammad Labib, Kejahatan Mayantara (Cyber crime), Refika Aditama, Bandung, 2005, Hal. 146)

Dokumen Elektronik yang memiliki muatan perjudian". 4)Penguntitan (Cyberstalking) Penguntitan tercantum dalam Pasl 29 UU Nomor 11 Tahun 2008 yang 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"

Pengaturan tentang penguntitan yang diatur dalam UU ITE sekilas mirip dengan pengaturan cyberstalking di beberapa negara, seperti Amerika Serikat, Kanada, dan Inggris yang dalam ketentuannya diatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan rasa takut, baik dengan kata- kata maupun tindakan tertentu. Perbuatan tersebut dilakukan dengan menggunakan atau melalui teknologi informasi dan komunikasi, misalnya dengan mail bombs, unsolicited mail, dan obsence or threatenig email.

5)Pemerasan/Pengancaman Pemerasan dan/atau pengancaman di cyber space dilarang dalam Pasal 27 ayat (4) UU Nomor 11 Tahun yang meyatakan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronok yang memiliki muatanpemerasan dan/atau pengancaman.

6)Ujaran Kebencian Tindakan ujaran kebencian diatur dalam Pasal 28 ayat (2) UU Nomor 11 Tahun 2008 yang menyatakan "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 antar golongan (SARA)".

7)Penyebaran berita bohong (hoax)

Penyebaran berita bohong diatur dalam Pasal 28 ayat (1) UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan "Setiap orang dengan sengaja dan tanpa(Sigid Suseno, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung, 2012, Hal. 177-178) hak menyebarkan berita bohing dan menyesarkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik".

8)Intersepsi Intersepsi diatur dalam Pasal 31 UU Nomor 19 Tahun 2016. Adapun perbuatan yang termasuk intersepsi adalah :

(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 atau transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersofat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun yang menyebabkan adanya perubahan, penghilangan dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditansmisikan. (3)Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

(4)Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang- undang.

Penjelasan yang dimuat dalam Pasal 31 ayat (1) yang dimaksud dengan intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau memcatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

9)Akses ilegal Akses ilegal dilarang dalam Pasal 30 UU Nomor 11 Tahun 2008 yang diatur dalam ayat :

(1)Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

(2)Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3)Setiap orang dengan sengaja dan tanpa hak atau melawan hukum menagakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

10)Kejahatan terhadap Informasi Elektronik/Dokumen Elektronik/ Data interference Kejahatan ini menjadikan Informasi Elektronik dan/atau Dokumen Elektronik sebagai sasaran dalam melakukan kejahatan yang diatur dalam Pasal 32 UU Nomor 11 Tahun 2008 dinyatakan sebagai berikut :

(1)Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau 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.

11)Gangguan terhadap sistem elektronik Gangguan terhadap sistem elektronik adalah kejahatan yang dilakukan dengan menyerang sistem sebagaimana yang diatur dalam Pasal 33 UU Nomor 11 Tahun 2008 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."

12)Penyalahgunaan perangkat Penyalahgunaan perangkat (*misuse of device)* merupakan tindakan yang melawan hukun yang diatur dalam Pasal 34 UU Nomor 11 Tahun 2008 dalam ayat :

(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 24 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

13)Pelanggaran yang terkait dengan komputer Pelanggaran terkait komputer biasanya digunakan untuk melakukan pemalsuan (forgery) dan penipuan (fraud). Dalam Pasal 35 UU Nomor 11 Tahun 2008 berbunyi "Setiap orang dengan sengaja dan tanpa hak 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."

2.Tinjauan Umum Tentang Cyber Crime

Istilah cyber crime saat ini merujuk pada suatu tindakan kejahatan yang berhubungan denga cyber space atau dunia maya dan tindakan kejahatan tersebut menggunakan komputer. Beberapa ahli yang menyakan antara tindak kejatan cyber dengan tindak kejahatan komputer, dan terdapat juga yang membedakan diantara keduanya.

Dalam beberaoa literatur, cyber crime sering di identikkan sebagai computer crime. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mengartikan cyber crime sebagai kejahatan di bidang computer. secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Menurut freddy haris, cyber crime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut : 1)Unauthorized access, 2)Unauthorized alteration or destruction of data, 3)Mengganggu/merusak operasi komputer, dan 4)Mencegah/mengahmbar akses pada komputer.

a.Kualifikasi *Cyber Crime*

Kualifikasi kejahatan dunia maya (*cyber crime*) sebagaimana dalam buku Barda Nawawi Arief, adalah kualifikasi (*cyber crime*) *menurut Convention on cybercrime* 2001 di Budapest Hongaria, yaitu :

1)*Illegal Interception* Sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.

2)Data *Interference* Sengaja dan tanpa hak melakukan perusakan, penghapusan,

perubahan atau penghapusan data komputer.

3)*System Interference* Sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.

4)*Misuse of Devive* Penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*).

5)*Computer Related Forgery* Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)

6)*Computer Related Fraud* Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

7)*Content-related offences* Delik-delik yang berhubungan dengan pornografi anak (child pornography)

8)*Offences related to infringements of copyright and related rights* Delik-delik yang terkait dengan pelanggaran hak cipta.

b.Jenis-jenis Tindak Pidana yang dilakukan dengan Cyber Crime

Dalam perkembangannya tindak pidana cyber crime memiliki berbagai jenis modus yang dilakukan da sering terjadi pada dunia maya :

1)Unauthorized Access 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 sistem jaringan komputer yang dimasukinya.Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun, begitu ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

2)Offense Against Intellecrual Property Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

3*)Illegal Contents*

Illegal contents 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.

4)*Cyberstalking*

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya

5)*Hacking dan Cracker*

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker.Dapat dikatakan bahwa *cracker* ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif.

6)*Cybersquatting dan Typosquatting Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada

perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

7)*Arp Spoofing*

Arp spoofing adalah teknik yang cukup populer untuk melakukan penyadapan data, terutama data username/password yang ada di jaringan internal. Intinya adalah dengan mengirimkan paket ARP Reply palsu sehingga merubah data MAC Address:IP yang ada di tabel ARP komputer target. Perubahan data ini menyebabkan pengiriman paket TCP/IP akan melalui attacker sehingga proses penyadapan dapat dilakukan.

8)*Carding*

Caring adalah berbelanja mengunakan nomor atau identitas kartu kredit orang lain yang dilakukan secara ilegal. Pelakunya biasa disebut carder.

9)*Defacing*

Defacing adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, BI baru-baru ini dan situs KPU saat pemilu 2004 lalu. Tindakan deface ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.

10)*Phising*

Phising adalah tindak kejahatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.

c.Kasus cyber crime yang terjadi di Indonesia

1)Pornografi

Awal Juni 2010 publik dikejutkan dengan munculnya tiga buah video mesum tiga artis ibu kota, yaitu Nazriel Irham (Ariel), Luna Maya dan Cut tari. Dalam pengakuannya Ariel mengatakan bahwa ia merasa kecolongan atas file pribadi yang diperuntukkan untuk dikonsumsi secara pribadi. Namun, hukum pun harus berjalan.

Ariel dijerat pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi dan Elektronik yang berbunyi: ""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". Ariel juga di jerat Pasal 29 UU Pornografi: Setiap orang yang memproduksi, membuat, memperbanyak menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksud. Majelis Hakim Pengadilan Negeri Bandung menjatuhkan hukuman 3,5 tahun penjara kepada Ariel dalam kasus video asusila tersebut.

Larangan melakukan perbuatan yang bermuatan melanggar kesusilaan diatur dalam Pasal 27 ayat (1) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal

27 ayat (1) menentukan: 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. Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (1) ditentukan dalam Pasal 45 ayat (1) yang berbunyi: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (5), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000.00 (satu miliar rupiah).

2)Defacing

Situs milik KPU (Komisi Pemilihan Umum) Defacing oleh hacker. Peristiwa tersebut terjadi pada tanggal 17 April 2004 dengan target situs http://tnp.kpu.go.id. Tampilan lambang 24 partai diganti dengan nama partai lucu „partai jambu", „partai cucak rowo", „Partai Kolor Ijo" dan lainnya.

Pelakunya, diketahui, bernama Dani Firmansyah 24 tahun mahasiswa asal Yogyakarta yang kemudian ditangkap Polda Metro Jaya. Motivasi pelaku, hanya ingin menjajal sistem pengamanan di server KPU yang dibeli sangat mahal dan anti bobol katanya saat itu ternyata berhasil di tembus oleh Dani.

Ketiadaan UU cyber di Indonesia membuat Dani Firmansyah dijerat dengan pasal-pasal Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengancam pidana terhadap perbuatan: "memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan eletromagnetik terhadap penyelenggaraan telekomunikasi".

Dani Firmansyah, juga dijerat melakukan tindak pidana yang melanggar pasal 22 huruf a, b, c, Pasal 38 dan Pasal 50 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi. Pada pasal 22 UU Telekomunikasi berbunyi: Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus. Sedangkan bunyi pasal 50 UU No 36/1999 tentang Telekomunikasi berbunyi "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)."

3)Pencemaran nama baik

Prita Mulyasari merupakan seorang pasien Rumah Sakit Omni Internasional Alam Sutra Tangerang. Kasus ini terjadi saat ia dirawat di Rumah Sakit tersebut Prita tidak mendapat kesembuhan namun penyakitnya malah bertambah parah. Pihak rumah sakit tidak memberikan keterangan yang pasti mengenai penyakit Prita, dan pihak Rumah Sakit tidak memberikan rekam medis yang diperlukan oleh Prita.

Kemudian Prita Mulyasari mengeluhkan pelayanan rumah sakit tersebut melalui email yang kemudian menyebar ke berbagai mailing list di dunia maya. Pihak Rumah Sakit Omni Internasional marah, dan merasa dicemarkan nama baiknya oleh Pita. Pihak RS Omni International mengadukan Prita Mulyasari secara pidana. Prita terjerat Undang-undang Nomor 11 Tahun 2008, Pasal 27 ayat (3) tentang Informasi dan Transaksi Elektronik (UU ITE).

Menurut banyak pakar. Tersangka tidak dengan Sengaja mau menghina atau mencemarkan nama baik karena ia hanya menyampaikan keluhan mengenai apa yang ia alami, Hak tersebut juga diatur dalam UU Perlindungan Konsumen." Prita punya hak untuk menyampaikan keluhan mengenai apa yang dialaminya. Karena Prita merupakan konsumen ia adalah pasien dari rumah sakit tersebut. Adanya

Kasus ini akan membawa dampak sangat buruk dan membuat masyarakat takut menyampaikan pendapat, kritik, saran atau komentarnya di dunia maya.

4)Peretasan situs negara

Peretasan Situs Negara www.presidensby.info, Pada 9 Januari

2013 situs www.presidensby.info di retas. Saat diretas, Halaman depan diganti dengan latar belakang hitam dengan tulisan warna hijau di bagian atas "Hacked by MJL007", sementara di bawahnya tertera sebuah logo dan tulisan "Jemberhacker Team" berwarna putih. Wildan ditangkap setelah melakukan deface situs SBY www.presidensby.info Wildan Yani S (22 th) peretas situs SBY lulusan SMK tahun 2010, Wildan memang tidak melanjutkan kuliah karena terhambat biaya.

Wildan ditangkap, terancam dengan melanggar Pasal 50 jo. Pasal 22 huruf b Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Wildan terancam hukuman pidana penjara paling lama 6 tahun penjara dan atau denda paling banyak Rp 600 juta. Wildan juga dinilai melanggar Pasal 46 Ayat (1), (2), dan (3) jo.

Pasal 30 Ayat (1), (2), dan (3) serta Pasal 48 Ayat (1) juncto Pasal 32 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Serangkaian pasal itu mengancam Wildan dengan hukuman penjara 6 hingga 10 tahun serta denda mencapai Rp 5 miliar.

3.Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Cyber Crime di Indonesia

a.Kebijakan RegulasiHukum Pidana Terhadap Tindak Pidana Teknologi Informasi Saat Ini Kebijakan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktivitas kehidupan manusia oleh karena itu dibutuhkan pengaturan secara khusus dengan dibentuknya suatu undang-undang yang dapat menanggulangi kejahatan terhadap teknologi informasi.

Peraturan terhadap teknologi informasi agar diterima masyarakat harus mempertimbangkan semua aspirasi (suprastruktur, infrastruktur, kepakaran dan aspirasi internasional) dan berbagai kepentingan harus diselaraskan dan diserasikan. Kebijakan hukum pidana (tataran aplikatif) sangat dipengaruhi sistem hukum yang berlaku saat ini. Hukum pidana Indonesia yang ada saat ini dan pengembangan ke depan dipengaruhi oleh tradisi hukum civil law.

Pembentukan peraturan perundang-undangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau cyber law akan bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

Sebelum diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan cybercrime tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan- perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-undang.8

Upaya menafsirkan cybercrime ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi telah dilakukan oleh penegak hukum dalam menangani cybercrime selama ini. Sebelum UU ITE diundangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan terobosan dengan penafsiran hukum yang berkaitan dengan teknologi

8. Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan informasi

khususnya kejahatan yang berkaitan dengan internet.

Dalam upaya menangani kasus kejahatan dunia maya, terdapat beberapa pasal dalam KUHP yang mengkriminalisasi cybercrime dengan mengggunakan metode interpretasi ekstensif (perumpamaan dan persamaan) terhadap pasal-pasal yang terdapat dalam KUHP. Adapun pasal-pasal yang dapat dikenakan dalam KUHP yang mengkriminalisasi terhadap kejahatan dunia maya, sebagaimana dikatakan oleh Petrus Reinhard Golose di antaranya adalah :

1)Pasal 362 KUHP untuk kasus Carding dimana pelaku mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di internet untuk melakukan transaksi di E- Commerce.

2)Pasal 378 KUHP untuk 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.

3)Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e- mail.

4)Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet

5)Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara on-line di internet dengan penyelenggara dari Indonesia.

6)Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di internet

7)Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.

Informasi, BPHN Departemen Kehakiman RI, 1995/1996, Hal. 32-34

8)Pasal 378 dan 262 KUHP dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan seolah- olah ingin membeli suatu barang dan membayar dengan kartu kredit yang nomor kartu kreditnya merupakan hasil curian.

9)Pasal 406 KUHP dapat dikenakan pada kasus deface suatu website, karena pelaku setelah berhasil memasuki website korban, selanjutnya melakukan pengrusakan dengan cara mengganti tampilan asli dari website tersebut.

Jaringan komputer yang menghasilkan cyberspace dan komunitas virtualnya berkembang seiring dengan berkembangnya kejahatan yang menghasilkan tindak pidana yang dianggap dahulu tidak mungkin pada saat sekarang ini menjadi mungkin bahkan dampaknya dapat dirasakan diluar tempat/wilayah negara. Oleh karena itu penerapan pasal-pasal KUHP sudah tidak relevan dalam penanggulangan tindak pidana teknologi informasi.

b.Upaya Penanggulangan Cyber Crime di masa yang akan datang Kurang optimalnya penegakan hukum terhadap cyber crimes disebabkan karena sarana dan fasilitas penegakan hukum yang belum memadai. Penegakan hukum terhadap cyber crime mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud. Penentuan waktu dan tempat terjadinya cyber crime ditentukan saat kapan alat itu bekerja efektif, oleh sebab itu analisis telematika sangat diperlukan dalam mengungkap kejahatan ini. Untuk menelusi, mendeteksi dan menanggulangi kejahatan ini Onno W. Purbo menjelaskan bahwa caranya sangat tergantung aplikasi dan topologi jaringan yang dipakai. Sebagian aplikasinya ada di gnacktrack dan backtrack.

Hal ini menggambarkan bahwa sarana dan fasilitas yang memadai menjadi hal yang penting dalam proses penegakan hukum. Tanpa adanya

sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi maka mustahil penegakan hukum akan mencapai tujuannya.

Pencegahan dan penanggulangan terhadap cyber crime membutuhkan pendekatan penal dan non penal yang integral dan membutuhkan keterpaduan. Membicarakan masyarakat adalah suatu keharusan atau kewajiban yang melekat pada perbincangan mengenai hukum. Hukum dan masyarakatnya merupakan dua sisi dari satu mata uang. Tanpa perbincangan mengenai masyarakat terlebih dahulu, sesungguhnya berbicara tentang hukum yang kosong. (Satjipto Rahardjo, 2009: 9). Satjipto Rahardjo menyimpulkan bahwa "setiap anggota masyarakat sebagai pemegang peranan ditentukan tingkah lakunya oleh pola-pola peraturan yang diharapkan daripadanya baik oleh norma-norma hukum maupun oleh kekuatan-kekuatan di luar hukum." (Satjipto Rahardjo, 2009: 27) Penegakan hukum berasal dari masyarakat dan bertujuan untuk mencapai kedamaian di dalam masyarakat. Oleh karena itu, dipandang dari sudut tertentu, maka masyarakat dapat mempengaruhi penegakan hukum tersebut. (Soerjono Soekanto, 2005: 45).

Untuk meningkatkan upaya penanggulangan kejahatan siber atau cyber crimes yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan cyber dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan cyber crime. Selain upaya dari kepolisian, kesadaran hukum masyarakat sangat diperlukan dalam berteknologi dan rendahnya kesadaran hukum para netter menjadikan penegakan hukum terhadap cyber crime tidak berjalan optimal. Tidak adanya kesadaran hukum para netter ini terlihat pada pemanfaatan sarana internet untuk melakukan berbagai jenis tindak pidana salah satunya memperjualbelikan layanan seks dan berbagai jenis tindak pidana lainnya.

Kesadaran hukum dari para korban untuk melaporkan kejahatan yang dialaminya masih sangat sedikit. Berdasarkan laporan Symantec bertajuk Norton Cybercrime Report, hampir satu dari dua (45 persen) korban kejahatan siber (cyber crime) tidak pernah menyelesaikan secara tuntas kejahatan siber yang mereka alami.

Kurangnya kesadaran hukum masyarakat berimplikasi dan pemahaman serta ketidaktaatan mereka terhadap hukum. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (lack of information) masyarakat terhadap jenis kejahatan cyber crime. Lack of information ini menyebabkan upaya penanggulangan cyber crime mengalami kendala, dalam hal ini kendala yang berkenaan dengan penaatan hukum dan proses pengawasan (controlling) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan cyber crime. Dengan demikian, kiranya tepatlah jika dikatakan bahwa penegakan hukum yang optimal memerlukan kesadaran hukum dan kesadaran moral dari masyarakat.

c.Faktor yang mempengaruhi dalam penanggulangan cyber crime di Indonesia

1)Faktor penanggulangan cyber crime melalui para penegak hukum

2)Solusi kebijakan hukum pidana terhadap penanggulangan cyber crime Terjadinya kasus cyber crime, pihak kepolisian telah melakukan berbagai upaya penanggulangan cyber crime upaya tersebut adalah upaya preventif dan represif.

a)Upaya preventif Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit cyber crime polisi telah

melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan broadcast berupa himbauan-himbauan terkait cyber crime untuk di forward ke masyarakat luas. Selain itu, dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara talkshow pihak kepolisian tidak henti-hentinya memberikan himbauan kemasyarakat.

b)Upaya represif Pihak kepolisian bekerja sama dengan stakeholder yang ada, yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus cyber crime, setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media dimana pihak media hadir untuk

4.Peran dari Virtual Police dan Cyber Police sebagai Aparat yang menangani masyarakat yang berpotensi melanggar UU ITE

a.Peran Yang Membedakan Virtual Police dengan Cyber Police

Dalam hal menangani dan menyelidiki cyber crime adalah peran dari cyber police dan virtual police. Peran dari virtual police sendiri adalah memberikan edukasi kepada masyarakat terkait dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE), sedangkan peran dari cyber police adalah menindaklanjuti kasus jika tindakan yang dilakukan oleh masyarakat tersebut tidak bisa ditegur oleh virtual police. Singkatnya virtual police muncul sebelum diselidiki lebih lanjur oleh cyber police.

Kehadiran virtual police ini cenderung masih baru di kalangan masyarakat diketahui pihak kepolisian sudah memiliki tim siber yang fungsinya tidak jauh berbeda dengan polisi virtual. Masih banyak masyarakat yang belum mengetahui perbedaan antara polisi virtual dan polisi siber, salah satu alasannya, yaitu kurangkan pengedukasian kepada masyarakat dengan cakupan yang lebih luas. Sejalan dengan hal ini, Koordinator Wilayah Peradi Jawa Tengah, Badrus Zaman menjelaskan perbedaan dari keduanya yaitu jika polisi virtual lebih mengedepankan upaya preventif, sedangkan polisi siber sudah pasti melakukan penegakan hukum sesuai regulasi yang ada karena polisi siber sudah dapat mendeteksi melanggar rambu-rambu UU ITE.

b.Penyidik Kepolisian terhadap Penyalahgunaan Informasi dan Transaksi Elektronik

Untuk mengetahui sejauh mana optimalisasi peran penyidik dalam proses penyidikantindak pidana penyalahgunaan informasi dan transaksi elektronik, maka pertama-tama harus dapat mengukur kinerja penyidik Kepolisian.

Berdasarkan Pasal 1 butir 5 KUHAP menegaskan penyelidikan adalah serangkaian tindakan/penyelidikan untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam Undang-undang. Penyelidikan dilakukan sebelum penyidikan. Dengan pengertian yang ditegaskan dalam KUHAP, penyelidikan sesungguhnya penyelidik yang berupaya atau berinisiatif sendiri untuk menemukan peristiwa yang diduga sebagai tindak pidana.Walaupun dalam pelaksaanan tugas penyelidikan terkadang juga menerima laporan atau pengaduan dari pihak yang dirugikan (Pasal 108 KUHAP). Tujuan dari pada penyelidikan memberikan tuntutan tanggung jawab kepada aparat penyelidik, agar tidak melakukan tindakan hukum yang merendahkan harkat dan martabat manusia.

Dengan memperhatikan rumusan Pasal 1 butir 5 KUHAP adalah Penyelidikan tersebut

dimaksudkan, untuk lebih memastikan suatu peristiwa itu diduga keras sebagai tindak pidana. Penyelidikan dimaksudkan untuk menemukan bukti permulaan dari pelaku (dader). Baik dalam Pasal 1 butir 5 maupun Pasal 5 KUHAP tidak ditegaskan perkataan pelaku atau tersangka. Dengan demikian, sudah tepat jika penyelidikan tersebut dimaksudkan untuk lebih memastikan suatu peristiwa yang diduga keras sebagai tindak pidana. Sedangkan penyidikan, sebagaimana ditegaskan dalam Pasal 1 butir 2 "serangkaian tindakan yang dilakukan pejabat penyidik sesuai dengan cara yang diatur dalam undang-undang ini (baca: KUHAP) untuk mencari serta mengumpulkan bukti dan dengan bukti itu membuat atau menjadi terang tindak pidana yang terjadi serta sekaligus menemukan tersangkanya atau pelaku tindak pidananya."

Tindakan penyelidikan penekanannya diletakkan pada tindakan mencari dan menemukan suatu peristiwa yang dianggap atau diduga sebagai tindak pidana. Pada penyidikan, titik berat tekanannya diletakkan pada tindakan mencari serta mengumpulkan bukti agar tindak pidana yang ditemukan dapat menjadi terang untuk menemukan dan menentukan pelakunya. Antara penyelidikan dan penyidikan adalah dua fase tindakan yang berwujud satu. Antara keduanya saling berkaitan dan isi mengisi guna dapat diselesaikan pemeriksaan suatu peristiwa pidana. Hal yang membedakan dari penyelidikan dan penyidikan sebagaimana dikemukakan oleh Yahya Harahap (2002:109) yaitu:

1)Dari segi pejabat pelaksana, pejabat penyelidik terdiri dari semua anggota POLRI dan pada dasarnya pangkat dan wewenangnya berada di bawah pengawasan penyidik.

2)Wewenang penyidik sangat terbatas, hanya meliputi penyelidikan atau mencari dan menemukan data atas suatu tindakan yang diduga merupakan tindak pidana. Hanya dalam hal-hal telah mendapat perintah dari pejabat penyidik, barulah penyelidik melakukan tindakan yang disebut Pasal 5 ayat 1 huruf b seperti penangkapan, larangan, meninggalkan tempat, penggeledahan dan penyitaan.

c.Faktor yang Menjadi Kendala Oleh Pihak Kepolisian Terhadap Tindak

Pidana Penyalahgunaan Informasi dan Transaksi Elektronik. Dalam upaya penanggulangan cyber crime oleh aparat kepolisian terdapat beberapa kendala yang menghambat upaya penanggulangan cyber crime, penulis kemudian memasarkannya berdasarkan hasil wawancara dan penelusuran referensi, bahwa penindakan kasus cybercrime sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka seringkali kita 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 komputer 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.

Hasil wawancara kepada kepala unit Rekrim bahwa kendala yang dihadapi oleh pihak penyidik Polrestabes Makassar dalam Penyidikan Tindak Pidana Cyber Crime adalah sebagai berikut:

1)Kendala Internal, kendala yang dihadapi adalah pada pelakunya saksi dari kasus serta tidak adanya unit khusus menangani masalah kejahatan dunia maya yang kita kenal dengan unit cyber crime, sementara pihak penyidik terkadang sulit mengetahui keberadaan pelaku sekalipun menggunakan teknologi

2)Kendala Eksternal, Izin ketua pengadilan untuk penggeledahan dan penyitaan serta izin melalui penuntut umum dari ketua pengadilan untuk

penangkapan dan penahanan, dan masyarakat yang kurang memahami masalah tindak pidana Cyber Crime dianggap sebagai bukan kejahatan.

D. PENUTUP

Pertama, penegakan hukum dalam penanggulangan cyber crime di Indonesia belum dilaksanakan secara optimal. Faktor-faktor yang akan mempengaruhi penegakan hukum terhadap cyber crimes meliputi faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas dalam penegakan hukum dan faktor masyarakat. Dari keempat faktor tersebut maka faktor yang paling berpengaruh pada lemahnya penegakan hukum yang ada terhadap penanggulangan cyber crimes dalam anatomi kejahatan transnasional adalah faktor hukum (substansi hukum) yang banyak mengandung kelemahan dan faktor penegak hukum.

Kedua, kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia cyber yang semakin canggih. Hal ini disebabkan tindak pidana teknologi informasi yang tidak mengenal batas-batas teritorial dan beroperasi secara maya. Oleh karena itu, menuntut pemerintah harus selalu berupaya mengantisipasi aktivitas-aktivitas baru yang diatur oleh hukum yang berlaku.

Ketiga, walaupun di Indonesia sudah terdapat aturan hukum yang mengatur tentang tindak pidana teknologi informasi secara jelas, haruslah aturan tersebut diperbarui seiring dengan perkembangan zaman yang semakin maju dan semakin banyaknya juga jenis cyber crime yang berbeda bentuknya yang mungkin akan terjadi di masa yang akan datang.

Keempat, pentingnya masyarakat dapat memahami dan dapat membedakan antara virtual police dan cyber police sebagai aparat yang ikut menanggulangi cyber crime. Kesadaran masyarakat akan hukum juga merupakan salah aspek penting untuk melaraskan tujuan agar tercapainya pemberantasan cyber crime yang marak terjadi.

E. DAFTAR PUSTAKA

Buku

Abdul Wahid & Mohammad Labib, Kejahatan Mayantara (Cyber crime), Refika Aditama, Bandung, 2005

Aloysius Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer, Universitas Atmajaya Yogyakarta, Yogyakatya, 1999

Barda Nawawi Arief, Kapita Selekta Hukum Pidana, PT. Citra Aditya Bakti, Bandung, 2003

Barda Nawawi Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Kencana Prenada Media Group, Jakarta, 2007

Mudadi & Barda Nawawi, Teori-teori dan Kebijakan Pidana, PT. Alumni Bandung, 2010

Sutarman, Cyber Crime Modus Operansi dan Penanggulangan,LaksBangPRESSindo, Yogyakarta, 2007

Sigid Suseno, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung, 2012

Soerjono Soekanto, Penelitian Hukum Normatif, Rajawali Press, Jakarta: 2006.

Jurnal/Tesis/Skripsi/Disertasi

Abdul Agis, Peranan Kepolisian Dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronik, Jurnal Al hikam, Vol. 1No. 2, 2017

Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi, BPHN Departemen Kehakiman RI, 1995/1996

Budi Kristian Rivanda Putra, Kebijakan Aplikasi Tindak Pidana Siber Di Indonesia, Journal of law, Vol. 1, 2018

Dwila Annisa & Mujiono Hafidh, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism, Jurnal Pembangunan Hukum Indonesia, Vol. 3 No. 2, 2021

Muhammad Muis, Kebijakan Hukum Pidana Dalam Penanggulangan Cyber Crime di Indonesia, Skripsi Universitas Muhammadiyah Sumatera Utara, Sumatera, 2019

Philemon Ginting, Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana, Tesis Universitas Diponegoro, Semarang, 2008

Refland, dkk, Tinjauan Yuridiis Efektivitas UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Jurnal Lex Crimen Vol.X/No.4, 2021

Rudi Hermawan, Kesiapan Aparatur Pemerintah Dalam Menghadapi Cyber Crime Di Indonesia, Jurnal Factor Exacta 6(1). 2013

Peraturan Perundang-Undangan:

Undang-Undang Dasar 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Infromasi dan Transaksi Elektronik.

Undang-Undang Nomor 16 Tahun 2016 tentang perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.