Nama : Meilyani Vica Ervita

Npm : 2012011032

Dosen Pengampu : Emilia Susanti, S.H.,M.H.

Mata Kuliah : Delik Khusus Di Luar KUHP

Resume

Tindak pidana ekonomi cyber crime dalam UU ITE terbaru

❖ Pengertian

Cyber crime adalah tindak pidana kriminal yang dilakukan pada teknologi internet, baik yang menyerang fasilitas umum di dalam cyberspace ataupun kepemilikan pribadi. Secara teknis tindak pidana tersebut dapat dibedakan menjadi offline crime, semi online crime, dan cybercrime. Masing-masing memiliki karakteristik tersendiri, namun perbedaan utama diantara ketiganya adalah keterhubungan dengan jaringan informasi publik. Cybercrime merupakan perkembangan lebih lanjut dari kejahatan atau tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer.

Fenomena cyber crime memang harus diwaspadai karena kejahatan ini sedikit berbeda dengan kejahatan lain. pada umumnya cyber Crime dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan.

Yang terjadi di internet terdiri dari berbagai macam jenis dan cara yang bisa terjadi. Bentuk atau model kejahatan teknologi informasi menurut motifnya kejahatan di internet dibagi menjadi dua motif yaitu :

1. Motif intelektual yaitu kejahatan yang dilakukan hanya untuk kepuasan diri pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi.
2. Motif ekonomi politik dan kriminal yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain.[1]

[1] https://repository.unikom.ac.id/

❖ Ruang Lingkup Tindak Pidana Ciber

Ada begitu banyak definisi cybercrimes, baik menurut para ahli maupun berdasarkan peraturan perundang-undangan. Definisi-definisi tersebut dapat dijadikan dasar pengaturan hukum pidana siber materil. Misalnya,

- Sussan Brenner (2011) membagi cybercrimes menjadi tiga kategori:

1. Kejahatan di mana komputer menjadi sasaran kegiatan kriminal
2. Kejahatan di mana komputer adalah alat yang digunakan untuk melakukan kejahatan,dan
3. Kejahatan di mana penggunaan komputer merupakan aspek insidental dari pelaksanaan kejahatan.

- Sedangkan, Nicholson menggunakan terminologi computer crimes dan mengkategorikan computer crimes (cybercrimes) menjadi objek maupun subjek tindak pidana serta instrumen tindak pidana.

1. Komputer mungkin menjadi 'objek' kejahatan:

   Pelaku menargetkan komputer itu sendiri. Ini mencakup pencurian waktu prosesor komputer dan layanan komputerisasi.

2. Komputer mungkin menjadi 'subjek' kejahatan:

   Komputer adalah situs fisik kejahatan, atau sumber, atau alasan, bentuk-bentuk unik kehilangan aset. Ini termasuk penggunaan 'virus', 'worm', 'Trojan horse', 'logic bombs', dan 'sniffer'.

3. Komputer mungkin menjadi 'instrumen' yang digunakan untuk melakukan kejahatan tradisional dengan cara yang lebih kompleks. Misalnya, komputer mungkin digunakan untuk mengumpulkan informasi kartu kredit untuk melakukan pembelian palsu.[2]

[2] https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia

- Menurut instrumen Perserikatan Bangsa Bangsa (PBB) dalam Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders yang diselenggarakan di Vienna, 10-17 April 2000, kategori cyber crime dapat dilihat secara sempit maupun secara luas, yaitu:

1. Kejahatan dunia maya dalam arti sempit ("kejahatan komputer"): setiap perilaku ilegal yang diarahkan melalui operasi elektronik yang menargetkan keamanan sistem komputer dan data yang diproses olehnya;
2. Kejahatan dunia maya dalam pengertian yang lebih luas ("kejahatan terkait komputer"): setiap perilaku ilegal yang dilakukan melalui, atau terkait dengan, sistem atau jaringan komputer, termasuk kejahatan seperti kepemilikan ilegal, menawarkan atau mendistribusikan informasi melalui komputer sistem atau jaringan.

- Convention on Cybercrime (Budapest, 23.XI.2001) tidak memberikan definisi cybercrime, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi:

1. Pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer
2. Pelanggaran terkait komputer
3. Pelanggaran terkait konten
4. Pelanggaran yang terkait dengan pelanggaran hak cipta dan hak terkait
5. Kewajiban tambahan dan sanksi Kewajiban Perusahaan

- Sementara dalam Black's Law Dictionary 9th Edition, definisi computer crime adalah sebagai berikut:

  Kejahatan yang melibatkan penggunaan komputer, seperti menyabotase atau mencuri data yang disimpan secara elektronik. - Disebut juga kejahatan dunia maya.[3]

[3] ibid

- Cyber crime diatur dalam Undang-Undang Transaksi Elektronik Nomor 8 Tahun 2011 sebagaimana telah diubah menjadiUndang- Undang Nomor 19 Tahun 2016, (“UU ITE”) khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam pasal 30 ayat (1), (2) dan (3) mengatakan bahwa:

    1. Dengan sengaja tanpa hak dan tanpa hak atau melawan hukum mengakses dan/ atau sistem elektronik orang lain dengan cara apapun,
    2. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem orang lain dengan cara apapun untuk tujuan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik,
    3. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan tujuan melanggar menerobos, melampaui, menjebol sistem pengaman[4]

- Sanksi bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa:

    - Ayat (1) :

      Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

    - Ayat (2) :

      Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

    - Ayat (3) :

      Dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).[5]

[4] https://www.legalku.com/jenis-jenis-cyber-crime-dan-perlindungan-hukumnya/#

[5] ibid

❖ Jenis-jenis Kejahatan Cyber Crime

Ada beberapa jenis kejahatan cyber crime yang harus menjadi perhatian masyarakat, antara lain:

1. Kejahatan Phising

[6]Phising adalah contoh cyber crime untuk melakukan penipuan dengan mengelabui korban. Umumnya aksi kejahatan ini dilancarkan melalui email maupun media sosial lain, seperti mengirimi link palsu, membuat website bodong, dan sebagainya.Tujuannya mencuri data penting korban, seperti identitas diri, password, kode PIN, kode OTP (one time password) pada akun-akun keuangan, seperti mobile banking, internet banking, paylater, dompet digital, sampai kartu kredit.

2. Kejahatan Carding

Carding adalah jenis kejahatan dunia maya yang dilakukan dengan bertransaksi menggunakan kartu kredit milik orang lain. Jadi, setelah mengetahui nomor kartu kredit korban, pelaku kemudian berbelanja online dengan kartu kredit curian itu.

Nomor kartu kredit tersebut dicuri dari situs atau website yang tidak aman. Bisa juga diperoleh dengan cara membeli dari jaringan spammer atau pencuri data. Selanjutnya data kartu kredit itu disalahgunakan oleh carder, sebutan pelaku kejahatan carding.

3. Serangan Ransomware

Ransomware adalah malware atau software jahat yang bukan hanya bisa menginfeksi komputer, tapi juga menyandera data pengguna. Tindak kejahatan ini dapat menimbulkan kerugian besar bagi korbannya.Pelaku akan meminta uang tebusan ke korban jika ingin ransomware dihapus atau dimusnahkan. Apabila korban tidak mengabulkan permintaan tersebut, pelaku tak segan-segan mengancam akan membuat data menjadi korup alias tidak bisa digunakan lagi.

.

[6] https://www.cermati.com/artikel/13-jenis-cyber-crime-kejahatan-internet-yang-merugikan

4. Penipuan online

Penipuan online atau penipuan digital yang saat ini makin banyak modusnya. Di antaranya adalah modus penipuan berkedok foto selfie dengan KTP atau identitas diri.Foto selfie bersama KTP biasanya menjadi salah satu syarat registrasi online akun keuangan, seperti dompet digital, paylater, pinjaman online, sampai daftar rekening bank online.

5. SIM Swap

SIM swap adalah modus penipuan dengan mengambilalih nomor ponsel atau kartu SIM ponsel seseorang. Tujuannya untuk meretas akun perbankan seseorang.Akibatnya, kartu SIM ponsel yang kemudian aktif dan berlaku adalah milik pelaku, bukan lagi punya korban. Oleh karena itu, jika ingin membuang kartu SIM lama, sebaiknya dipatahkan atau digunting agar tidak disalahgunakan orang lain.[7]

6. Peretasan situs dan email

Kejahatan ini istilahnya deface website dan email. Yakni jenis kejahatan cyber crime dengan cara meretas sebuah situs ataupun email, serta mengubah tampilannya.Dengan kata lain, penampilan website atau email kamu mendadak berubah akibat peretasan ini.Contoh, halaman situs bukan yang biasanya, jenis huruf ganti, muncul iklan tidak jelas, bahkan mencuri data yang kamu tidak menyadarinya.

7. Kejahatan Skimming

Jenis kejahatan cyber crime lain yang harus diwaspadai, yakni skimming. Skimming adalah kejahatan perbankan dengan cara mencuri data kartu debit atau kartu kredit untuk menarik dana di rekening.Cara kerjanya membobol informasi pengguna memakai alat yang dipasang pada mesin Anjungan Tunai Mandiri (ATM) atau di mesin gesek EDC. Dengan teknik tersebut, pelaku bisa menggandakan data yang terdapat dalam pita magnetik di kartu kredit maupun debit.Kemudian memindahkan informasi ke kartu ATM kosong. Akhirnya, pelaku bisa dengan mudah menguras saldo rekening nasabah.Skimming dapat terjadi ketika kamu sedang transaksi belanja online. Saat kartu debit atau kartu kredit terhubung pada gawai, risiko terkena skimming menjadi lebih tinggi.Ponsel atau laptop terkoneksi dengan internet sehingga memudahkan pelaku meretas atau mengambil data kartu kredit atau kartu debit. Terlebih jika

[7] https://www.cermati.com/artikel/13-jenis-cyber-crime-kejahatan-internet-yang-merugikan

menggunakan koneksi wifi publik. Jadi, pastikan setiap transaksi online pakai jaringan internet pribadi.

8. OTP Fraud

OTP (One Time Password) adalan Kode sekali pakai yang sangat vital untuk keamanan bertransaksi.Kode OTP ini ibarat kunci. Kunci akhir untuk bisa mengakses atau menyelesaikan transaksi keuangan. Jika kode 6 digit ini sampai diketahui orang lain, bisa berbahaya.Saat ini, marak kejahatan pencurian kode OTP atau OTP fraud. Penyebab OTP fraud adalah malware atau semacam virus yang menyerang perangkat lunak.Penyebab lainnya bisa juga melalui aplikasi, social engineering seperti via telepon, SMS, email. Contohnya lewat call center palsu.[8]

9. Pemalsuan Data atau Data Forgery

Jenis kejahatan cyber crime Indonesia berikutnya adalah data forgery. Adalah kejahatan dengan memalsukan data atau dokumen penting melalui internet. Biasanya kejahatan ini menyasar pada dokumen penting milik - e-commerce atau penyedia situs belanja online. Seolah-olah terjadi salah ketik yang merugikan pengguna atau masyarakat.

10. Kejahatan konten ilegal

Divisi Hubungan Internasional Polri juga menyebut konten ilegal termasuk dalam jenis kejahatan cyber crime. Konten ilegal adalah kejahatan memasukkan data atau informasi yang tidak benar, tidak etis, melanggar hukum atau mengganggu ketertiban umum.

Sebagai contoh, berita bohong atau fitnah, pornografi, maupun informasi yang menyangkut rahasia negara, propaganda untuk melawan pemerintah yang sah.

11. “Teroris” Dunia Maya atau Cyber Terorism

Cyber terorism adalah kejahatan yang mengganggu, atau membuat kerusakan terhadap suatu data di jaringan komputer. Pelaku menawarkan diri kepada korban untuk memperbaiki data tersebut yang sudah disabotase dengan bayaran tertentu.

[8] https://www.cermati.com/artikel/13-jenis-cyber-crime-kejahatan-internet-yang-merugikan

12. Mata-mata atau Cyber Espionage

Jenis kejahatan cyber crime yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer korban.Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.

13. Menjiplak Situs Orang Lain

Kejahatan melanggar Hak Atas Kekayaan Intelektual (HAKI) orang lain di internet. Misalnya meniru tampilan situs orang lain secara ilegal, menyiarkan informasi yang merupakan rahasia dagang orang lain.[9]

- Perlindungan hukum terhadap korban tindak pidana penipuan melalui internet

  Perkembangan teknologi selain membawa dampak positif, dalam perkembangannya juga membawa dampak negatif. [10]Kejahatan penggunaan internet sebagai sarana untuk melakukan kejahatan telah meningkat secara substansial di Negara Indonesia sebagai bentuk dampak negatifnya. Internet digunakan sebagai sarana untuk melakukan kejahatan, salah satunya adalah penipuan. Perlindungan yang diberikan oleh Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik berupa penyelesaian perkara dan pemberian sanksi pidana yang diberikan kepada tersangka atau terdakwa. Pasal 28 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dapat diindikasikan sebagai pasal yang mengatur tentang penipuan, namun jika ditelaah lebih dalam, unsur-unsur yang terkandung dalam Pasal 28 ayat (1) UU - Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dinilai masih kurang memenuhi unsur-unsur yang

[9] https://www.cermati.com/artikel/13-jenis-cyber-crime-kejahatan-internet-yang-merugikan

[10] https://jurnal.hukumonline.com/a/5cb49aaa01fb73000e1c74ce/perlindungan-hukum-terhadap-korban-tindak-pidana-penipuan-melalui-internet

terkandung dalam undang-undang yang memberikan informasi fiktif dalam hal penjualan barang di dunia maya.

Lain halnya dengan Pasal 378 KUHP, yang merinci unsur-unsur perbuatan yang memberikan keterangan fiktif.

Dalam perlindungan hukum terhadap korban cybercrime secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan :

[11]

1). Model Hak-hak Prosedural (The Procedural Rights Model)

Pada model hak prosedural, korban kejahatan cybercrime diberikan hak untuk melakukan tuntutan pidana atau membantu jaksa, atau hak untuk dihadirkan pada setiap tingkatan peradilan diamana keterangannya dibutuhkan, secara implisit dalam model ini korban diberikan kesempatan untuk “membalas” pelaku kejahatan yang telah merugikannya. Dalam model prosedural itu korban juga diminta lebih aktif membantu aparat penegak hukum dalam menangani kasusnya apalagi berkaitan dengan kejahatan yang modern cybercrime. Dengan adanya hak prosedural juga dapat menimbulkan kembali kepercayaan korban setelah dirinya dirugikan oleh mereka yang tidak bertanggungjawab (terdakwa), disamping itu hal ini juga dapat menjadi pertimbangan bagi jaksa dalam hal apabila jaksa membuat tuntutan yang terlalu ringan.

2). Model Pelayanan (The Service Model)

Model pelayanan ini bertitik berat terletak pada perlunya diciptakan standar-standar baku bagi pembinaan korban kejahatan cybercrime. Model ini melihat korban sebagai sosok yang harus dilayani oleh Polisi dan aparat penegak hukum yang lain, pelayanan terhadap korban cybercrime oleh aparat penegak hukum apabila dilakuakan dengan baik akan membawa dampak positif bagi penegakan hukum ksususnya cybercrime, dengan demikian korban perkembangan teknologi ini akan lebih percaya institusi penegak hukum dengan adanya pelayanan terhadap korban, dengan demikian maka korban akan merasa haknya dilindungi

[11] https://media.neliti.com/media/publications/43295-ID-perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia.pdf

dan dijamin kembali kepentingannya. Pada proses persidangan, terutama yang berkenaan dengan pembuktian kejahatan dunia maya, banyak kasus yang terjadi akibat perkembangan teknologi informasi hal ini mengharuskan aparat penegak hukum menyiapkan sumber daya manusia yang handal dan mengerti dab paham dengan teknologi. mengingat kejahatan cybercrime merupakan kejahatan modern yang harus mendapat perhatian yang serius dari pemerintah, karena kejahatan di dunia maya akan berimbas pada dunia nyata.

Pentingnya perlindungan hukum bagi korban kejahatan cyber, selain dalam kerangka mewujudkan negara hukum, hal ini penting dilakukan sebagai suatu tindakan preventif yang dilakukan oleh aparat penegak hukum dalam mengurangi ataupun mencegah terjadinya korban kejahatan dunia maya dan tentunya bukan hanya sebagai penampung laporan akan tetapi yang diharapkan adalah adanya tindakan nyata dari aparat penegak hukum sehingga masyarakat pengguna teknologi benar-benar merasa aman dalam melakaukan aktifitasnya di dunia maya.

- Pengaturan Tindak Pidana Ciber Materil di Indonesia

  Sebagai sebuah negara hukum sudah merupakan suatu kewajiban negara melindungi setiap warga negaranya dari setiap perbuatan yang dapat merusak ataupun merugikan masyarakat, salah satunya yaitu perlindungan hukum yang diberikan oleh negara terhadap masyarakat pengguna teknologi, hukum dan teknologi adalah dua kata yang berbeda akan tetapi saling mempengaruhi dan juga dapat mempengaruhi kehidupan masyarakat itu sendiri. [12]

- Pengaturan tindak pidana ciber di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang **menggunakan sarana atau dengan bantuan sistem elektronik.** Itu artinya semua tindak pidana konvensional dalam **Kitab Undang-Undang Hukum Pidana ("KUHP")** sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana

[12] https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia

siber dalam arti luas. Demikian juga tindak pidana dalam **Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana ("UU 3/2011")** maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam **Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang ("UU TPPU").**

Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 19/2016")** sama halnya seperti Convention on Cybercrimes, UU ITE juga tidak memberikan definisi mengenai cybercrimes, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada Convention on Cybercrimes (Sitompul, 2012):

a. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:

1). Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:[13]

- Kesusilaan (Pasal 27 ayat (1) UU ITE);

  "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".

- Perjudian (Pasal 27 ayat (2) UU ITE);

  "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".

- penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE);

[13] https://media.neliti.com/media/publications/43295-ID-perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia.pdf

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik”.

- pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE);

  “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”

- berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE);

  “setiap orang dengan sengaja dan tanpa hakmenyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”

- menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);

  “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)”

- mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

  “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.

2). Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE);[14]

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

b) 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.

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

3). intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU 19/2016);

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.

b. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

1). Gangguan terhadap Informasi atau Dokumen Elektronik (data interference - Pasal 32 UU ITE);

“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). Gangguan terhadap Sistem Elektronik (system interference –Pasal 33 UU ITE)

“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”

[14] ibid

c. . Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);[15]

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, menggandakan untuk digunakan, mengimpor, mendristribusikan, menyediakan, atau memiliki:

a) Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana yang 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 yang dimaksud dalam Pasal 27 sampai dengan Pasal 33.

d. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);

“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”.

e. Tindak pidana tambahan (accessoir Pasal 36 UU ITE);

“setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampaai dengan Pasal 34 yang mengakibatkan kerugian pada orang lain”

f. Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE)

Di samping itu, dalam UU ITE juga mengatur ketentuan pidana yang sangat berat bagi pelaku kejahatan dunia maya yang diatur dalam Pasal 45 sampai dengan Pasal 52 adapun ancaman pidananya mulai dari 6 (enam) tahun sampai dengan 12 (dua belas) tahun penjara dan denda mulai dari Rp. Rp 600.000.000,00 (enam ratus juta rupiah) sampai dengan Rp 12.000.000.000,00 (dua belas miliar rupiah).

[15] ibid

❖ **Pengaturan Tindak Pidana Ciber Formil di Indonesia**[16]

Selain mengatur tindak pidana ciber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. **Pasal 42 UU ITE** mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam **Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP") dan ketentuan dalam UU ITE**. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

a. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika;

b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;

c. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana;

d. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

[16] https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia

Adapun prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut:

1. Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian Cybercrime atau kepada penyidik PPNS pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam UU ITE.
2. Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPNS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI.

Selain UU ITE, peraturan yang menjadi landasan dalam penanganan kasus cybercrime di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.[17]

Dengan adanya aturan matril maupun formil yang mengatur tentang kejahatan di dunia maya setidaknya dapat membantu aparat penegak hukum dalam menangani kejahatan yang terjadi di dunia maya baik kejahatan yang konvensional maupun kejahatan modern. Dengan harapkan dapat memberikan rasa aman bagi masyarakat pengguna teknologi informasi mengingat kejahatan teknologi ini tidak mengenal ruang dan waktu dan dapat terjadi pada siapa saja dan kapan saja

[17] https://media.neliti.com/media/publications/43295-ID-perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia.pdf