UNES LAW REVIEW
+62 822 8750 4359
+62 822 8750 4359
https://review-unes.com/
uneslawreview@gmail.com

DOI: https://doi.org/10.31933/unesrev.v3i1
Diterima: 28/09/2020, **Diperbaiki:** 20/10/2020, **Diterbitkan:** 04/11/2020

TINJAUAN PERISTIWA *CYBER CRIME* YANG TERJADI PADA TAHUN 2019 DI KOTA SAWAHLUNTO

Yumelfi Futra
Polsek Barangin Sawahlunto, Sumatera Barat, Indonesia
Email: yumelfifutra@gmail.com

***Corresponding Author*: Yumelfi**

ABSTRACT

Cyber Crimeis a form of virtual crime by utilizing computer which connected to the internet network, and exploiting other devices or computers that is connected to the internet. Cybercrime was previously regulated in the regulation Number 36 Year 1999 concerning Telecommunications, however this regulation has not been able to accommodate virtual and computer crimes. To anticipate the development of information technology, regulation Number 19 Year 2016 concerning Amendments to regulation Number 11 of 2008 concerning Electronic Information and Transactions was issued. In Sawahlunto City in 2019, several cyber-crime incidents were found, such as online extortion, fraud through online , and theft of Wi-Fi wireless streams, therefore a research was conducted on how the cyber-crime events that occurred in Sawahlunto City in 2019 , regulations governing cyber, the causes and obstacles in handling the cyber-crime. The data used are secondary supporting data collected through library research and primary data as supporting data which is carried out through field studies with interview techniques. The results showed that: the discovery of cyber-crimes that occurred in Sawahlunto City in 2019 such as online extortion, online fraud and theft of Wi-Fi wireless streams, knowing the regulations on cyber-crime, namely the ITE Regulation and knowing the factors and obstacles in handling cyber-crimes that occurred in the City Sawahlunto in 2019.

Kata Kunci: Tinjauan Peristiwa, Cyber Crime, Kota Sawhlunto

PENDAHULUAN

Indonesia merupakan negara yang mempunyai banyak keberagaman maupun kebudayaan, keberagaman tersebut secara nyata tidak terlepas dari Telekomunikasi dan Informasi sebagai sarana pemanfaatan agar secara mudah dapat mengetahui apa saja keberagaman yang ada di indonesia, maupun diluar Indonesia. Perkembangan yang dinilai pesat dalam masa dekat ini dari bidang teknologi telekomunikasi dan komputer terjadi pada sub bidang seperti material dan perangkat lunak, seperti transaksi perangkat lunak beberapa sektor yaitu e-*banking, e-commerce, e-trade, e-bussines dan e-realiting* (Andi Hamzah, 1990:23-24).

Pada mulanya sistem telekomunikasi dan informatika merupakan dua sistem kerja yang berbeda yang bekerja parsial. Sistem telekumunikasi dilakukan dengan memancarkan (*taransmission*) suatu pesan atau data dengan signal elektronik dari suatu tempat si pengirim (*origin*) dan kesuatu tempat si penerima informasi (*destination*), baik melalui suatu medium kabel maupun jalur gelombang radio (*radio link*) ataupun signal radio (*radio signl*) (Edomon makarim, 2004:47).

Perkembangan yang pesat dalam pemanfaatan telekomunikasi seperti Intenet diperhatikan dalam beberapa waktu ini banyak mengundang terjadinya kejahatan. Kejahatan pada sistem teknologi infomasi dan komputer merupakan salah satu kejahatan yang termasuk kategori *Cyber Crime*, yang mana *Cyber Crime* disebut juga kejahatan dunia maya adalah salah satu bentuk kejahatan Virtual dengan memanfaatkan media komputer yang terhubung dengan jaringan internet, dan mengeksploitasi perangkat lain ataupun komputer yang terhubung dengan internet juga.

Fakta menunjukkan bahwa Internet melahirkan perubahan karakter sosial dan budaya masayarakat. Perubahan karakter tersebut mengantarkan masyarakat pada pola "pengingkaran hakikat kemanusiaan manusia", sebagai makhluk tuhan yang berakal. Dampaknya dapat diprediksiakn bahwa masyarakat semakin tidak terkendali hingga menyentuh titik kriminalitas dari apa yang diperoleh dari perkembangan telematika atau internet termasuk peristiwa yang terjadi di Kota Sawahlunto dengan bebrbagai peristiwa yang berkaitan dengan *cyber* (Maskun, 2014:10).

METODE PENELITIAN

Metode penelitian yang penulis gunakan adalah analisis yuridis dengan penelitian normatif. Penelitian normatif adalah suatu penelitian yang dilakukan terhadap data-data yang berupa "*Law In Book*". Bentuk penelitian normatif adalah suatu bentuk penelitian dengan melihat studi kepustakaan, dilakukan dengan cara menelusuri atau menelaah dan menganalisis bahan pustaka atau bahan dokumen siap pakai. Dalam penelitian hukum, bentuk ini dikenal sebagai *legal research*, dan jenis data yang diperoleh disebut data sekunder. Kegiatan yang dilakukan dapat berbentuk menelusuri dan menganalisis peraturan, mengumpulkan dan menganalisis vonis atau yurisprudensi, membaca dan menganalisis kontrak ataumencari, membaca dan merangkum dari suatu buku acuan. Metode pengumpulan data yang akan penulis lakukan dalam penulisan ini adalah dengan cara melakukan penelitian kepustakaan yang meliputi (Pedoman Penyusunan Usulan Penelitian dan Tesis, 2017:6) **:**

a. Bahan Hukum Primer yaitu KUHP, KUHAP dan UU Khusus yang berkaitan dengan Telekomunikasi, Infromasi Elektronik, Komputer (*cyber*).
b. Bahan Hukum Sekunder yaitu buku - buku serta bahan hukum yang menjelaskan bahan hukum primer yaitu berupa penjelasan Undang-Undang.
c. Bahan Hukum Tersier yaitu bahan hukum yang berkaitan dengan bahan hukum primer dan sekunder, misalnya wacana dari internet dan meneliti peristiwa yang terjadi terkait *cyber*.

HASIL DAN PEMBAHASAN

Pengertian *Cyber* dan *Cyber Crime* beberapa Ahli

Sebelum menjelaskan lebih jauh tentang pengertian kejahatan *cyber*, Telematika ataupun sejenisnya, dirasa perlu untuk menyatukan pendapat tentang apa yang dimaksud dengan kejahatan telematika. Dilihat dari literaturnya *cyber (cyber sapace*) atau dunia maya adalah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal balik secara online.

Apakah kejahatan telematika dapat disamakan dengan kejahatan komputer (*computer crimes*) atau kejahatan siber (*cyber crime*) atau kejahatan baru yang dikenal dalam kepustakaan teknologi dan informasi. Di dasari dari beberapa literatur pada argumentasi bahwa *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik dial up sistem, jalur telepon, maupun *wireless system* makan konvergensi ini disebut dengan telematika.

Sehingga jika menyebutkan kejahatan telematika, maka yang dimaksud juga adalah *cyber crime*. Akan tetapi disisi lain, beberapa pakar tetap berpendapat bahwa baik kejahatan komputer, kejahatan *cyber*, maupun kejahatan telematika adalah kejahatan yang sama dengan penamaan yang berbeda, seperti pengertian *cyber crime* menurut beberapa ahli :

1. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer", mengartikan bahwa *Cyber Crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara Ilegal.
2. *Forester* dan *Morrison* mendefeniskan kejahatan komputer merupakan aksi kriminal dimana komputer dijadikan sebagai senjata utama.
3. Girasa mendefeniskan *Cyber Crime* sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama.
4. M. Yoga P memeberikan defenisi *Cyber Crime* yaitu kejahatan dimana tindakan kriminal hanya bisa terjadi disunia *cyber*.
5. Menurut *Organization of European Community Development* (EOCD) kejahatan dunia maya atau *cyber crime* adalah semua akses ilegal terhadap suatu transmisi data. Artinya, semua kegiatan akses ilegal terhadap suatu transmisi data. Artinya, semua kegiatan yang tidak sah dalam suatu sistem komputer termasuk suatu tindak kejahatan.

Metode Kejahatan *Cyber Crime*

Maraknya jenis *Cyber Crime* saat ini maka metode dalam melakukanya cukup beragam. Berikut ini adalah beberapa cara kerja atau metode *Cyber Crime* yang sering dilakukan ;

1. *Password Cracker*

   Ini adalah suatu tindakan mencuri password orang lain dengan menggunakan suatu program yang dapat membuka enkripsi password. Tindakan ini juga sering dilakukan untuk menonaktifkan suatu sistem pengamanan password.

2. *Spoofing*

   Spoofing adalah tindakan memalsukan data atau identitas seseorang sehingga pelaku (*hacker*) dapat melakukan login ke dalam sutu jaringan komputer layaknya user yang asli.

3. DDoS (*Distributed Denial of Sevice Attack*)

   Ini adalah serangan yang dilakukan terhadap komputer atau server di dalam jaringan internet yang dilakukan oleh seseorang *hacker/attacker*. Serangan DDoS akan menghabiskan sumber daya (*resource*) yang ada pada suatu komputer atau server, hingga tidak dapat lagi menjalankan fungsi dengan benar.

4. *Sniffing*

   Sinffing adala bentuk *Cyber Crime* dimana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai Akun korban untuk melakukan penipuan atas nama korban atau merusak/menghapus data milik korban.

5. *Destructive Devices*

   Ini adalah Program atau *Software* berisikan Virus dimana tujuannya adalah untuk merusak atau menghancurkan data-data di dalam komputer korban. Beberapa yang termasuk dalam program adalah *Worms, Trojan Horse, Nukes, Email Bombs*, dan lain-lain.

Jenis-Jenis *Cyber Crime*

Modus Operandi dan berkembangnya tindak pidana *Cyber Crime* cukup beragam, sehingga Jenis-jenis tindak pidana *Cyber Crime* semakin banyak. Adapun Jenis tindak pidana *Cyber Crime* sesuai dengan bentuk peristiwa, yakni ;

1. Jenis *Cyber Crime* berdasarkan Motif ;
   a) *Cyber Crime* sebagai tindak kejahatan murni :

      Dimana orang yang melakukan kejahatan yang dilakukan secara disengaja. Sebagai Contoh yaitu Pencurian, Tindakan Anarkis terhadap suatu sistem informasi atau sistem komputer.

   b) *Cyber Crime* sebagai tindakan kejahatan abu-abu :

      Dimana kejahatan ini jelas antara kriminla atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

   c) *Cyber Crime* yang menyerang individu :

      Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, Contoh : Pornografi dan *Cyber Stalking.*

   d) *Cyber yang* menyerang Hak Cipta (Hak Milik) :

      Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi atau tidak materi.

e) *Cyber Crime* yang menyerang Pemerintah :

Kejahatan yang dilakukan terhadap pemerintah sebagai Objek motif melakukan Teror, membajak atau merusak keamanan terhadap sistem *Cyber* pemerintah.

2. Jenis *Cyber Crime* berdasarkan aktivitas ;

a) *Unauthorized Access to Computer Sistem and Service* :

Kejahatan ini dilakukan dengan memasuki/menyusup kedalam suatu sistem jaringan komputer secara tidak sah atau tanpa izin. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting

b) *Cyber Crime* berupa *Ilegal 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. Sebagai contoh adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri seseorang.

c) *Data Forgery*:

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

d) *Cyber Espionage* :

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer sasaran.

e) *Cyber Sabotage* dan *Extortion* :

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

f) *Offense Intelectual Property* :

Kejahatan ini ditunjukkan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Segabai contoh adalah peniruan tampilan pada *Web Page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang seseorang atau perusahaan.

3. Jenis *Cyber Crime* berdasarkan Sasaran ;

a) *Cyber Crime* yang menyerang Individual (*Againts Person*) :

Jenis kejahatan ini menentukan serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai dengan tujuan penyerangan tersebut. Contoh : Pornografi dan *Cyber Stalking*.

b) *Cyber Crime* menyerang hak milik (*Againts Property*) :

Cyber yang dilakukanuntuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan ini seperti mengakses komputer secara tidak sah melalui *Cyber Space*, pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding*, *cybersquatting*, dan *hijacking*.

c) *Cyber Crime* menyerang Pemerintah (*Againts Goverment*) :

Cyber Crime *Againts Goverment* dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan ini misalkan *Cyber Terorism* sebagai tindakan yang mengancam pemerintah juga *cracking* ke situs resmi Pemerintah, Lembaga maupun Militer.

Pengaturan Tindak Pidana *Cyber* di Indonesia

1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *Cyber Crime*. Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *Cybercrime*. Namun undang-undang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *Cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomudir tindak-tindak pidana yang berkaitan dengan komputer.

"Pasal 22 yang berbunyi: "Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi : 1) Akses ke jaringan telekomunikasi; dan atau 2) Akses ke jasa telekomunikasi; dan atau 3) Akses ke jaringan telekomunikasi khusus."

"Pasal 38 yang berbunyi : "Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi"

"Pasal 40 yang berbunyi : "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun".

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamnanya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime*.

2. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Tanggal 23 April 2008 telah diundangkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini bukanlah undang-undang tindak pidana khusus, melainkan juga memuat tentang pengaturan mengenai pengelolaan informasi dan transaksi elektronik dengan tujuan pembangunan, namun undang-undang ini juga mengantisipasi pengaruh buruk dari pemanfaatan kemajuan teknologi ITE

tersebut, yakni dengan diaturnya hukum pidana khususnya tentang tindak pidana yang menyerang kepentingan hukum orang pribadi, masyarakat, atau kepentingan hukum Negara dengan memanfaatkan kemajuan teknologi ITE, atau sering disebut tindak pidana *cyber crime*.

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang ITE (*cybercrime*) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana *cybercrime* dalam UU ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35. Pada 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Sementara ancaman pidananya ditentukan di dalam Pasal 45 sampai Pasal 52. Adapun rumusan pasal-pasal tersebut adalah sebagai berikut:

"Pasal 27 yang berbunyi :

1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.
3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

"Pasal 28 yang berbunyi:

1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
2) Setiap orang dengan sengaja dan tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA)."

"Pasal 29 yang berbunyi: "Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."

"Pasal 30 yang berbunyi:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

"Pasal 31yang berbunyi:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/ atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah."

"Pasal 32 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

"Pasal 33 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya."

"Pasal 34 yang berbunyi:

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

"Pasal 35 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

"Pasal 36 yang berbunyi: " Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain."

"Pasal 37 yang berbunyi: "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia."

Dari uraian rumusan pasal-pasal bentuk-bentuk tindak pidana *Cyber Crime* menurut Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diklasifikasikan menjadi 2 bentuk yakni:

a. *Cyber Crime* yang menggunakan komputer sebagai alat kejahatan, yakni Pornografi Online (*Cyber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui computer, pemerasan dan pengancaman melalui komputer, penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, *Cyber Terrorism*.

b. *Cyber Crime* yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*Illegal Acces*), menggangu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Perbutan yang dilarang dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sama dengan perbuatan yang dilarang dengan Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik tidak ada penambahan maupun pengurangan tindak pidana tersebut yang diancam pemidanannya, sehingga bentuk-bentuk *Cyber Crime* masih sama dengan undang-undang sebelumnya. Perbedaan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah sebagai berikut :

a. UU No 11 Tahun 2008 tentang ITE :

Dalam Pasal 1 mengenai ketentuan umum terdapat 23 poin ketentuan-ketentuan umum.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Dirubah dengan penambahan dalam Pasal 1 yakni Pasal 1 diantara angka 6 dan angka 7 disipkan 1 angka yakni angka 6a, ketentuan mengenai Penyelenggara Sistem Elektronik.

b. UU No 11 Tahun 2008 tentang ITE :

Rumusan pasal mengenai bentuk-bentuk tindak pidana.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Rumusan bentuk-bentuk tindak pidana ITE masih tetap sama dengan UU sebelumnya tidak ada penambahan rumusan pasal mengenai perbuatan yang dilarang hanya terdapat perubahan dalam pasal 31.

c. UU No 11 Tahun 2008 tentang ITE :

Tidak adanya penjelasan mengenai Pasal 5 tentang alat bukti elektronik.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Dirubah dengan penambahan penjelasan dalam Pasal 5.

d. UU No 11 Tahun 2008 tentang ITE :

Tidak adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan.

e. UU No 11 Tahun 2008 tentang ITE :

Segala bentuk penyadapan tidak diperbolehkan.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Penyadapan boleh dilakukan dalam rangka penegakan hukum atas permintaan kepolisian dan kejaksaan.

f. UU No 11 Tahun 2008 tentang ITE :

Dalam hukum acara yang digunakan ada ketentuan khusus dalam hal pengeledahan, penyitaan barang bukti yakni mutlak harus melalui izin pengadilan.

UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE :

Adanya perubahan dalam penggeledahan dan penyitaan barang bukti elektronk dilakukan sesuai dengan ketentuan hukum acara pidana dalam KUHAP.

Peristiwa Tindak Pidana *Cyber Crime* di Kota Sawahlunto.

Kejahatan Dunia Maya akhir-akhir ini cukup menjadi perhatian di Indonesia dikarenakan cukup banyak modus dan jenis laporan yang diterima dalam *Cyber Crime* langsung di alami masyarakat. Berikut ada beberapa contoh kasus *Cyber Crime* yang terjadi di Kota Sawahlunto, yaitu ;

a. Kasus yang diterima di Polres Sawahlunto pada bulan Januari tahun 2019, melaporkan bahwa seorang Gadis menjadi korban peristiwa penipuan melalui aplikasi Pencari Jodoh di internet. Tiga bulan sebelum peristiwa penipuan ini di laporkan oleh Pelapor inisial (NK) berjenis kelamin Perempauan, NK mengakses aplikasi Pencarian Jodoh "*Love time.com dan Jodoh Sakinah.com*". Pada aplikasi tersebut NK berkenalan dengan sesorang laki-laki bernama inisial (JM). Kemudian NK dan JM melanjutkan komunikasi melalui Media Sosial lainnya maupun melalui Alat Komunikasi Telepon, NK dan JM menjalin hubungan asmara pacaran tanpa pernah bertemu langsung dan setelah 2 Bulan komunikasi, NK mengirimkan uang dalam jangka waktu 1 minggu kepada JM berjumlah Rp. 60.000.000,-.

   NK menerangkan bahwa uang yang dikirim digunakan oleh JM untuk persiapan Pernikahan, namun satu bulan setelah NK mengirimkan uang, JM tidak dapat dihubungi dan tidak bisa berkomunikasi sampai NK melaporkan peristiwa tersebut ke Polres Sawahlunto. Personil Polres Sawahlunto melakukan penyelidikan terkait laporan NK, dan menemukan peristiwa Tindak Pidana sesuai Pasal 378 dan 372 KUHPidana terhadap laporan NK. Selanjutnya JM ditetapkan sebagai Tersangka, kemudian dilakukan Penyidikan sampai ketahap peradilan.

b. Pada bulan Desember tahun 2019 seorang laki-laki berinisial NP mendatangi Kantor Polsek Barangin Polres Sawahlunto, NP melaporkan tentang Pencurian Internet Wifi di Wireless miliknya. Sesuai laporan NP bahwa Pencurian Daya Internet Wifi miliknya sering dilakukan

oleh beberapa pemuda yang berada di dekat rumahnya. Sebelumnya NP pernah menegur beberapa orang pemuda yang memakai Internet WiFi nya tersebut dan meminta agar tidak menggunakannya lagi, namun para pemuda tersebut tidak menghiraukan teguran NP.

Karena tidak dihiruakan oleh beberapa pemuda yang sering membobol Wireless miliknya, NP melaporkan peristiwa tersebut ke Polsek Barangin. Pada peristiwa tersebut Personil Polsek Barangin menemukan beberapa kendala dalam hal Penyidikan, namun pada hasil penyelidikan intensif diduga pelaku pembobol Wireless milik NOPER yaitu dengan menggunakan Aplikasi yang ada pada Gatget milik diduga pelaku, seperti Aplikasi *"Router Keygen, Wifi Password Hcker Prank dan Wifi Master Key"*.

Faktor-Faktor Terjadinya Tindak Pidana Kejahatan Dunia Maya/*Cybercrime*

Modus Operandi dan berkembangnya tindak pidana Dunia Maya cukup pesat sehingga bentuk-bentuk tindak pidana *cyber crime* semakin banyak. Hal ini dipengaruhi oleh beberapa faktor. Adapun beberapa faktor terjadinya tindak pidana *cyber crime*, yakni ;

1. Kesadaran Hukum Masyarakat

   Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. *Cybercrime* adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum. Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *Cybercrime* kurang. Hal ini disebabkan anatara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahtan *Cybercrime*. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvesional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya, sehingga hal tersebut membuat kejahatan tersebut meningkata dan meluas akibatnya.
2. Faktor Keamanan

   Rasa aman tentunya akan dirasakan oleh pelaku kejahatan *Cybercrime* pada saat sedang menjalankan aksinya. Hal ini tidak lain karena internet lazim dipergunakan di tempat-tempat yang relatif tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan dan warung internet. Aktivitas yang dilakukan oleh pelaku di tempat tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya pada saat pelaku sedang melakukan tindak pidana sangat jarang orang luar mengetahuinya. Hal ini, sangat berbeda dengan kejahatan-kejahatan yang sifatnya konvensional, yang mana pelaku akan mudah diketahui secara fisik ketika sedang melakukan aksinya. Sehingga rasa aman yang diperoleh dalam melakukan tindak pidana tersebut membuat tindak pidana *cybercrime* terjadi terus menerus dan meningkat.
3. Faktor Penegak Hukum

   Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*Cybercrime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti

yang dapat dipakai menjerat pelaku. Sehingga tak jarang jika pelaku dapat lolos dari jeratan hukum dan tindak pidana tersebut semakin banyak.

4. Faktor Sosial Ekonomi

   Faktor ini juga mempengaruhi maraknya tindak pidana *cybercrime* karena isu global yang kemudian dihubungkan dengan kejahatan tersebut sebenarnya merupakan masalah keamanan jaringan (*security network*). Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang sangat membutuhkan perangkat keamanan jaringan. *Cyber Crime* berada dalam skenario besar dalam kegiatan ekonomi dunia, sosialekonomi yang meningkat membuat celah-celah pelaku dalam menjalankan aksinya.

5. Faktor Globalisasi

   Adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain sehingga memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat dari pada yang lain. Akses internet yang tidak terbatas. Dengan akses internet yang tidak terbatas pengguna internet dengan bebas mengakses situs-situs yang ada di internet sehingga hal ini menimbulkan adanya pelaku *cybercrime* dengan cara *download, upload* dan lain sebagainya secara illegal atau tidak sah.

KESIMPULAN

1. Untuk dapat mewujudkan peraturan perundang-undangan yang efektif di bidang Transaksi dan Komunikasi Informasi Elektronik maka diperlukan komitmen politik, peraturan perundang-undangan yang proporsional, intelijen di bidang Informasi yang kuat, pengawasan sektor Informasi, penegakan hukum, dan kerjasama dalam berbagai bidang Telematika baik di dalam maupun luar Negara.
2. Masih lemahnya peraturan Undang-undang yang mengatur tindak pidana di dunia maya, dan faktor ini yang dapat dimanfaatkan oleh para pelaku tindak pidana dunia maya untuk mencari celah-celah hukum agar lolos dari jerat hukum.
3. Kelemahan lain ada pada perangkat digital forensik (lab komputer forensik mabes Polri) yang belum dimiliki secara menyeluruh oleh Polri di setiap daerah, mengingat penting keberadaannya dalam mencegah, maupun menangani kasus-kasus yang berkaitan dengan Cyber Crime dan Telematika.

DAFTAR PUSTAKA

Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1990

Edomon makarim, *Kompilasi Hukum Telematika*, Grafindo Persada, Jakarta, 2004

Maskun, S.H,.LLM, *Kejahatan Siber Cyber Crime*, Prenada Media Group, Jakarta, 2014

Pedoman Penyusunan Usulan Penelitian dan Tesis, Universitas Ekasakti, Padang, 2017

Undang-Undang Nomor 1 Tahun 1946 Tentang Kitab Undang-Undang Hukum Pidana,

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi,

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik (ITE),

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik (ITE).

https://www.kompasiana.com/nabilah_cw/5a0cfbeefcf6811a8712b7d3/dunia-cyber-dunianya-calon-kejahatan?page=all, di akses Minggu tanggal 03 November 2019

http://ogapermana.blogspot.com/2013/04/pengertian-cyber-crime-menurut-para-ahli_11.html, di akses Minggu tanggal 03 November 2019

https://www.maxmanroe.com/vid/teknologi/pengertian-cybercrime.html, diakses Minggu tanggal 03 November 2019

http://ogapermana.blogspot.com/2013/04/pengertian-cyber-crime-menurut-para-ahli_11.html, di akses Minggu tanggal 03 November 2019