Dampak Pengaruh Teknologi Terhadap (Cyber Crime) Tindak Pidana Serta Analisis Hukum Terkait

Faturohman
Fakultas Hukum, Universitas Bina Bangsa
email : arturcikaseban@gmail.com
Rachmat Putra Hidjriana
Fakultas Hukum, Universitas Bina Bangsa
email : rachmatph55@gamail.com
Rizky Zendra Rahayu
Fakultas Hukum, Universitas Bina Bangsa
email : rizkirendra22@gmail.com

Abstract

Technology that fundamentally changes the way we interact and transact, also has a significant impact on cyber crime. In preparing the journal, we carried out an in-depth analysis of the influence of modern technology, such as artificial intelligence, blockchain, and the Internet of Things, on the increasing incidence of cyber crime. It found that continued technological innovation creates new opportunities for cybercriminals, while unaddressed security weaknesses increase the risk of attacks. A deep understanding of these dynamics is key to developing effective and proactive solutions to combat cybersecurity challenges in today's digital era. Legal and cyber security constraints that have not been able to keep up with the pace of technological development are the main causes of the increasing number of cyber crimes. Therefore, a deep understanding of the relationship between technology and cybercrime is very important to formulate effective security strategies in this digital era.

Keywords: Technology, Cyber Crime, Legal Obstacles.

Abstrak

Teknologi yang mengubah secara fundamental cara kita berinteraksi dan bertransaksi, juga memberikan dampak signifikan terhadap kejahatan siber (cyber crime). Dalam penyusunan jurnal, kami melakukan analisis mendalam terhadap pengaruh teknologi modern, seperti kecerdasan buatan, blockchain, dan Internet of Things, terhadap meningkatnya insiden cyber crime. Ditemukan bahwa keberlanjutan inovasi teknologi menciptakan peluang baru bagi pelaku kejahatan siber, sementara kelemahan keamanan yang belum teratasi meningkatkan risiko serangan. Pemahaman mendalam terhadap dinamika ini menjadi kunci untuk mengembangkan solusi yang efektif dan proaktif dalam melawan tantangan keamanan siber di era digital saat ini.

Kendala hukum dan keamanan siber yang belum mampu menyusul laju perkembangan teknologi menjadi penyebab utama faktor utama angka kejahatah cyber kian meningkat. Oleh karena itu,pemahaman mendalam terhadap hubungan antara teknologi dan kejahatan siber sangat penting untuk merumuskan strategi keamanan yang efektif di era digital ini.

Kata Kunci : Teknologi, Cyber Crime, Kendala Hukum.

Pendahuluan

Kemajuan ilmu pengetahuan dan tekhnologi telah memberikan dampak yang sangat positif bagi peradaban umat manusia. Salah satu fenomena abad modern yang sampai saat ini masih terus berkembang dengan pesat adalah internet. Pada mulanya jaringan internet hanya dapat digunakan oleh lingkungan pendidikan (perguruan tinggi) dan lembaga penelitian.

Kemudian tahun 1995, internet baru dapat digunakan untuk publik, beberapa tahun kemudian tim Berners-Lee mengembangkan aplikasi Word Wide Web (WWW) yang memudahkan orang untuk mengakses informasi di internet. Setelah dibukanya internet untuk keperluan publik semakin banyak muncul aplikasiaplikasi bisnis di internet. Perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar tekhnologi informasi, dalam penelitiannya yang dikutip oleh harian Kompas menyatakan "Kejahatan cyber (cyber crime) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para hacker yang rata-rata anak muda yang keliatannya kreatif, tetapi sesunggunya mereka mencuri nomor kartu kredit melalui internet. Kejahatan cyber crime dibagi menjadi 2 kategori, yakni cyber crime dalam pengertian sempit dan dalam pengertian luas. cyber crime dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan cyber crime dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.3 Istilah–istilah yang tetap digunakan tersebut tetap diarahkan pada pengertian kejahatan terhadap komputer *(Crime directed at computer),* kejahatan dengan mendayagunakan komputer *(Crimes utilizing computers),* atau kejahatan yang berkaitan dengan komputer *(Crimes related to computer),* walaupun istilah-istilah tersebut belum memberikan gambaran–gambaran yang tepat. Meskipun demikian, istilah apapun yang digunakan, berbagai pihak telah berusaha membuat definisinya sendiri– sendiri berdasarkan pemahamannya. Dalam hal ini terdapat tiga pendekatan untuk mempertahankan keamanan di cyberspace, per tama adalah pendekatan

teknologi, ke-dua pendekatan sosial budaya-etika, dan ke-tiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga cyber crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP "Nullum delictum nulla poena sine praevia lege poenali" atau dalam istilah lain dapat dikenal, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu".

Perkembangan tekhnologi yang sangat pesat, membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan tekhnologi tersebut. Sayangnya, hingga saat ini banyak negara belum memiliki perundangundangan khusus di bidang tekhnologi informasi, baik dalam aspek pidana maupun perdatanya.

Kerangka Pemikiran

Menurut Van Hamel memberikan definisi tindak pidana (strafbaar feit)yaitu kelakuan orang (menselijke gedraging) yang telah dibentuk dalam undang-undang (wet), bersifat melawan hukum, yang turut dipidana (strafwaardig) dan dilakukan atas kesalahan. Kejahatan di bidang teknologi informasi atau dapat disebut cyber crime makin marak di Indonesia. Ketentuan hukum pidana yang mengatur kejahatan di bidang teknologi informasi lazim disebut *cybercrime law*. Jika berbicara terkait hukum pidana pasti tidak bisa dilepaskan dari hukum pembuktian.

Hukum pembuktian itu sendiri adalah seperangkat kaidah hukum yang mengatur tentang pembuktian.Pembuktian dalam ilmu hukum adalah suatu proses, baik dalam acara perdata maupun acara pidana, maupun acara-acara lainnya, dengan menggunakan alat-alat bukti yang sah, dilakukan tindakan dengan prosedur khusus, untuk mengetahui apakah suatu

fakta atau pernyataan, khususnya fakta atau pernyataan yang dipersengketakan di pengadilan, yang diajukan dan dinyatakan oleh salah satu pihak dalam proses pengadilan itu benar atau tidak seperti yang dinyatakan itu. Sistem pembuktian dalam acara pidana dikenal dengan "system negative" (negatief wettelijk bewijsleer), artinya yang dicari oleh hakim adalah kebenaran materil. Yangdimaksud dengan sistem negatif, yang merupakan sistem yang berlaku dalam hukum acara pidana, adalah suatu sistem pembuktian di depan pengadilan agar suatu pidana dapat dijatuhkan oleh hakim, haruslah memenuhi dua syarat mutlak, yaitu:

1. Alat bukti yang cukup,
2. Keyakinan hakim Dengan demikian,

Tersedianya alat bukti saja belum cukup untuk menjatuhkan hukuman pada seorang tersangka. Sebaliknya, meskipun hakim sudah cukup yakin akan kesalahan tersangka, jika tidak tersedia alat bukti yang cukup, pidana belum dapat dijatuhkan hakim.Sistem pembuktian negatif ini diakui berlakunya secara eksplisit oleh Kitab Undang-Undang Hukum Acara Pidana, melalui Pasal 183. Selengkapnya, Pasal 183 tersebut menyatakan sebagai berikut: "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila sekurang-kurangnya dua alat bukti yang sah, ia memperoleh keyakian bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya." Sistem pembuktian negatif dalam sistem pembuktian pidana diberlakukan karena yang dicari oleh hakim-hakim pidana adalah suatu kebenaran materil *(materiele waarheid).*

Perkembangan dalam sistem hukum pembuktian khususnya yang menyangkut dengan pembuktian elektronik, setelah keluarnya Undang-Undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik. Alat bukti elektronik berupa informasi elektronik, dokumen elektronik, dan hasil cetaknya dengan tegas diakui sebagai diakui sebagai alat bukti yang sah dan penuh di pengadilan asalkan memenuhi persyaratan tertentu sebagaimana yang ditentukan dalam undang-undang.8 Penggunaan alat bukti elektronik dalam sistem hukum pembuktian didasari atas asas-asas sebagai berikut :

a) Asas kepastian hukum;
b) Asas manfaat;
c) Asas kehati-hatian;
d) Asas itikad baik; dan
e) Asas kebebasan memilih teknologi atau netral teknologi.

Selanjutnya, pengakuan hukum pembuktian terhadap penggunaan dan pemanfaatan alat bukti elektronik dari teknologi informasi dan transaksi elektronik di Indonesia adalah sebagai berikut :

a. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
b. Meningkatkan perdagangan dan perekonomian nasional melalui bisnis dengan menggunakan e-commerce.
c. Meningkatkan efektivitas dan efisiensi pelayanan publik.
d. Memajukan pemikiran dan kemampuan masyarakat di bidang pemanfaatan teknologi informasi.
e. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna jasa teknologi informasi.

Metodelogi

Adapun metode yang digunakan dalam penelitian adalah sebagai berikut:

a. Jenis Penelitian Jenis penelitian yang digunakan adalah deskriptif, yaitu untuk memberikan gambaran yang selengkap-lengkapnya mengenai upaya pembuktian oleh aparat penegak hukum dalam rangka mencari kebenaran materiil dalam perkara pidana cyber crime baik secara yuridis maupun empirisnya.
b. Metode Pendekatan Metode pendekatan yang diterapkan dalam penelitian ini adalah yuridis empiris.Pendekatan ini mengkaji konsep normatif atau yuridis mengenai upaya pembuktian oleh aparat penegak hukum dalam mencari kebenaran materiil dalam perkara pidana cyber crime sesuai dengan peraturan perundangundangan yang berlaku dan pelaksanaannya di masyarakat.
c. Jenis Data Dalam penelitian ini penulis akan menggunakan sumber data sebagai berikut:
    1. Data Primer Data primer adalah data yang diperoleh langsung dari sumber data di lapangan dengan mengadakan wawancara secara langsung dengan responden di lokasi penelitian.
    2. Data Sekunder yautu Data berupa bahan-bahan pustaka yang terdiri dari:
        a. Bahan hukum primer, meliputi:
            - Kitab Undang-undang Hukum Pidana (KUHP)
            - Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

- Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi
- Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia
- Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Peraturan Perundang-undangan lainnya yang terkait dengan pengaturan dunia maya (cyber space)

b. Bahan Hukum Sekunder, meliputi literatur-literatur yang terkait dengan tindak pidana dunia maya (cyber crime)
c. Bahan Hukum Tersier, meliputi bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder. Adapun petunjuk yang digunakan adalah kamus hukum.
d. Metode Pengumpulan Data Untuk mengumpulkan data yang dimaksud di atas digunakan teknik sebagai berikut:
   - Studi Kepustakaan

     Dilakukan dengan mencari, mencatat, menginventarisasi, menganalisis, dan mempelajari data yang berupa bahan-bahan pustaka.

   - Analisis Situasi

     Situasi yang di cerna dalam penulisan ini ialah beberapa sebab yang terjadi kian hari karena makin maraknya situasi kejahatan yang disebabkan basis teknologi yang makin modern sehingga menyebabkan pelaku tindak kejahatan cyber makin banyak jumlahnya.

Identifikasi Masalah

Cybercrime atau biasa disebut kejahatan telematika sudah tidak asing ditelinga masyarakat kita. Cybercrime seringkali dihubungkan dengan banyak kasus seperti kasus pembobolan ATM di beberapa bank di Indonesia, masalah terorisme, bahkan sampai kepada kasus pornografi. Banyak hal yang melatar belakangi kasus-kasus tersebut serta banyak hal pula yang mengancam stabilitas keamanan internasional. Dengan kata lain, ada kasus pasti harus ada penyelesaiannya. Dalam makalah ini, penulis juga akan menguraikan siapa saja yang aktor terlibat dalam kasus-kasus tersebut, siapa saja yang harus berperan dalam menanggulangi masalah cybercrime, dan peraturan perundang-undangan seperti apa yang diterapkan di beberapa negara seperti Amerika Serikat dan juga di Indonesia. Makalah ini hanya akan membahas beberapa hal di bawah ini

1. Bagaimanakah sifat kejahatan telematika sebagai kejahatan transnasional?
2. Bagaimanakah pendekatan prinsip-prinsip yurisdiksi dalam hukum internasional dalam mengantisipasi dan menangani kejahatan telematika sebagai kejahatan transnasional?
3. Dengan cara bagaimana masyarakat internasional dapat mengantisipasi dan menangani kejahatan telematika tersebut?

Pembahasan

1. Definisi Kejahatan Transnasional

Secara konseptual, transnational crime atau kejahatan transnasional adalah tindak pidana atau kejahatan yang melintasi batas negara. Konsep ini diperkenalkan pertama kali secara internasional di tahun 1990-an dalam The Eigth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.

Sebelumnya isitilah yang telah lebih dulu berkembang adalah organized crime. PBB sendiri menyebut organized crime sebagai the large-scale and complex criminal activity carried on by groups of persons, however loosely or tightly organized, for the enrichment of those participating and at the expense of the community and its members Pada perkembangannya PBB menambahakan bahwa istilan ini seringkali diartikan sebagai the large-scale and complex criminal activities carried out by tightly or loosely organized. associations and aimed at the establishment, supply and exploitation of illegal markets at the expense of society.

Menurut United Nations Convention on Transnational Organized Crime tahun 2000, kejahatan dapat dikatakan bersifat transnasional jika terdiri dari:

a. dilakukan di lebih dari satu negara,
b. persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain,
c. melibatkan organized criminal group dimana kejahatan dilakukan di lebih satu negara, dan
d. berdampak serius pada negara lain. Kejahatan transnasional merupakan fenomena sosial yang melibatkan orang, tempat dan kelompok, yang juga dipengaruhi oleh berbagai sosial, budaya, faktor ekonomi.

Akibatnya, berbagai negara cenderung memiliki definisi kejahatan transnasional yang sangat berbeda tergantung pada filosofi tertentu. Menurut Martin dan Romano, *transnational crime may be defined as the behavior of ongoing organizations that involves two or more nations, with such behavior being defined as criminal by at least one of these nations.*

Berdasarkan beberapa uraian diatas, menurut saya kejahatan transnasional merupakan kejahatan yang terjadi antar lintas negara yang dapat dikategorikan sebagai kejahatan yang terorganisasi dengan baik dan penuh dengan perencanaan matang. Dalam setiap peristiwa kejahatan transnasional aktornya tidak selalu berkaitan dengan nation-state actor, melainkan individu, dan kelompok. Dalam setiap aksinya para mereka tidak hanya berperan sebagai pelaku tetapi juga sebagai penyumbang dana maupun pikiran untuk melancarkan aksinya. Latar belakang kejahatan ini juga cukup luas, menyangkut bidang politik, ekonomi, sosial, budaya, agama, dll. Bannyak juga kejahatan transnasional yang tidak terkait dengan latar belakang tersebut.

Suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional atau bukan dapat dilihat dari:

a. melintasi batas negara,
b. pelaku lebih dari satu, bisa nation-state actor ataupun yang lain,
c. memiliki efek terhadap negara ataupun aktor internasional (misalnya individu ±dalam pandangan kosmopolitan) di negara lain,

d. melanggar hukum di lebih dari satu negara, Pada tahun 1995, PBB telah mengidentifikasi 18 jenis kejahatan transnasional, yaitu pencucian uang, terorisme, pencurian benda seni dan budaya, pencurian kekayaan intelektual, perdagangan senjata gelap, pembajakan pesawat, pembajakan laut, penipuan asuransi, kejahatan komputer, kejahatan lingkungan, perdagangan orang, perdagangan bagian tubuh manusia, perdagangan narkoba, penipuan kepailitan, infiltrasi bisnis, korupsi, dan penyuapan pejabat publik atau pihak tertentu.

2. Karakteristik Cyber Crime

Berdasarkan motif kegiatannya, kejahatan telematika (cyber crime) dapat digolongkan kedalam:

a. Kejahatan kerah biru (blue collar crime)
   Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokkan, pencurian, pembunuhan dan lain-lain.
b. Kejahatan kerah putih (white collar crime)
   Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu. Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model di atas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal berikut:
   a) Ruang lingkup kejahatan
   b) Sifat kejahatan
   c) Pelaku kejahatan
   d) Modus Kejahatan
   e) Jenis kerugian yang ditimbulkan

3. Upaya Penanggulangan di Indonesia Oleh POLRI

Dalam artikel yang ditulis oleh Kombes (Pol) Drs. Petrus Reinhard Golose, M.M, ia mengungkapkan bahwa terdapat beberapa Undang-Undang terkait dengan Cybercrime (kejahatan telematika) yang berlaku di Indonesia, antara lain:

a. Kitab Undang Undang Hukum Pidana Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada cybercrime antara lain :
   - Pasal 362 KUHP yang dikenakan untuk kasus carding dimana pelaku mencuri nomor 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. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

- Pasal 378 KUHP dapat dikenakan 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. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.
- Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.
- Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.
- Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.
- Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negri dimana pornografi yang menampilkan orangdewasa bukan merupakan hal yang ilegal.
- Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus Sukma Ayu-Bjah.
- Pasal 378 dan 262 KUHP dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
- Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta. Menurut Pasal 1 angka (8) Undang- Undang No 19 Tahun 2002 tentang Hak Cipta, program computer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam

merancang intruksi-intruksi tersebut. Hak cipta untuk program computer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/ software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp20.000,00.

Penjualan dengan harga sangat murah dibandingkan dengan software asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping. Maraknya pembajakan software di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program computer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/ atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah) ".

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi Menurut Pasal 1 angka (1) Undang-Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tandatanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau system elektromagnetik lainnya.

   Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang-Undang ini, terutama bagi para hacker yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

   1) Akses ke jaringan telekomunikasi
   2) Akses ke jasa telekomunikasi
   3) Akses ke jaringan telekomunikasi khusus

Kesimpulan

Analisis hukum tentang tindak pidana cybercrime menekankan pentingnya penyesuaian peraturan hukum dengan perkembangan teknologi. Diperlukan upaya untuk memperkuat perlindungan hukum terhadap korban cybercrime, meningkatkan kapasitas penegakan hukum, dan mendorong kerjasama internasional dalam menanggulangi ancaman keamanan digital. Implementasi peraturan yang efektif dapat memberikan landasan yang kokoh dalam menindak dan mencegah tindak pidana di dunia maya.

Jurnal analisis hukum tentang tindak pidana cybercrime ini menyoroti urgensi reformasi hukum yang menyeluruh dalam menghadapi tantangan keamanan digital. Diperlukan penyusunan undang-undang yang lebih adaptif terhadap perkembangan teknologi, peningkatan kapasitas penegakan hukum, serta kerjasama internasional yang erat. Kesadaran hukum dan

pemahaman masyarakat terhadap risiko cybercrime perlu ditingkatkan, sementara penegakan hukum harus dapat mengakomodasi kompleksitas serangan digital. Hanya dengan pendekatan komprehensif ini, sistem hukum dapat memberikan perlindungan yang efektif terhadap individu dan entitas yang menjadi korban tindak pidana di dunia maya.

Cybercrime atau kejahatan telematika adalah tergolong kejahatan transnasional (transnational crime) karena dalam mejalankan aksinya aktor cybercrime (hacker) memanfaatkan teknologi internet sebagai media utama. Saat ini cybercrime telah menjadi masalah tidak hanya bagi satu negara tapi hampir seluruh negara, karena sifatnya yang transnasional. Cybercrime juga dapat digolongkan kedalam berbagai macam seperti kasus pornografi, teroris, pembobolan ATM dan lain sebagainya. Dalam peanggulangan secara global banyak poin-poin kesepakatan dari hasil konvensi-konvensi tersebut yang menghasilkan peraturan-peraturan cybercrime yang harus dipatuhi oleh masyarakat dunia. Di Indonesia, dengan berlakunya Undang-Undang Nomor 11 tahun 2008 mengenai Informasi dan Transaksi Elektronik, maka kita berharap agar Indonesia tidak lagi menjadi "safe heaven" bagi pelaku kejahatan telematika. Hal ini juga harus didukung oleh peningkatan pengetahuan atas teknologi informasi dan komunikasi baik dari para aparat penegak hukum misalnya polisi, hakim dan jaksa, juga adanya sosialisasi terhadap masyarakat berkaitan dengan kejahatan telematika itu sendiri.

Daftar Pustaka

David Berlind, "Reno's Border Patrol Made Ineffective," PC Week, April 8, 1996, hlm. 78.

Garda T. Paripurna, Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional, 2008, Gerhard O. W. Mueller,

Transnational Crime: Definitions and Concepts, Transnational Organized Crime 4, no. 1998 (n.d.). Havana, Cuba 27 August to 7 September 1990, A/Conf.144/7, 26 July 1990. John R. Wagley, Transnational Organized Crime:Principal Threats and U.S. Responses (Congressional Research Service, The Library of Congress, 2006).

Mark Findlay, The globalization of Crime: Understanding Transnational Relationship in Context (Cambridge University Press, 2003).

Martin, J. M. and Romano, A. T., Multinational Crime-Terrorism, Espionage, Drug & Arms Trafficking (SAGE Publications, 1992 Melissa Virus Exposes Computer Users' Vulnerability," Japan Computer Industry Scan, April 12, 1999,available at 1999 WL 9642279; Muladi, Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, 1st ed. (Jakarta: The Habibie Center, 2002).

Richard Power, ed., 2000, "2000 CSI/FBIComputerCrime and Security Survey," Computer Security Issues and Trends 6, hlm. 3 See "Hackers Alter Romanian Money Rate," New York Times on the Web/ Breaking News from United Nations, Changes in Forms and Dimensions of Criminality - Transnational and National, Working paper prepared by the Secretariat for the Fifth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Toronto, Canada, 1-12 September 1975).

Suspected Russia Hackers Held," New York Times on the Web/Breaking News from Associated Press, United Nations, Eigth United Nations Congress on the Prevention of Crime and the Treatment of Offende