Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia

Miftakhur Rokhman Habibi-Isnatul Liviani

rokhmanhabibi@uinsby.ac.id | *UIN Sunan Ampel*
Jl. A. Yani 117 Surabaya, Indonesia

Abstract: This article aims to let us learn more about cyber crime. This is due to the weakness of cyberspace can become a global disaster that threatens the business sector, national and global security, behavior, child protection, and government systems. The results showed that the public is currently still misusing social media to spread crime in cyberspace. Most of the perpetrators of cybercrime on social media will be caught by Law No.11 of 2008 concerning Electronic Information and Transactions (UU ITE), whether intentional or unintentional. The law should provide protection for internet users with good intentions, and provide firm action for perpetrators of cyber crime. However, the legal system has not solved all computer crimes over the Internet. Likewise in the investigation, there were many obstacles related to legal instruments, the ability of investigators, evidence, and computer forensic facilities. This is why cyber crime law enforcement is still weak.
Keywords: Cyber crime, Criminal policy, Information technology

Abstrak: Artikel ini bertujuan agar kita dapat mempelajari lebih lanjut tentang kejahatan dunia maya. Ini dikarenakan bahwa kelemahan dunia maya dapat menjadi bencana global yang mengancam sektor bisnis, keamanan nasional, perilaku, perlindungan anak, dan sistem pemerintahan. Hasil penelitian menunjukkan bahwa masyarakat saat ini masih menyalahgunakan media sosial untuk menyebarkan kejahatan di dunia maya. Sebagian besar pelaku kejahatan dunia maya di media sosial akan di jerat oleh Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), baik disengaja maupun tidak disengaja. Hukum semestinya mempersembahkan perlindungan terhadap pengguna internet dengan niat yang baik, dan memberikan tindakan tegas bagi para pelaku cyber crime. Namun, sistem hukum belum menyelesaikan semua kejahatan komputer melalui Internet. Begitu pula dalam penyidikannya, terdapat banyak kendala yang berkaitan

dengan perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Inilah mengapa penegakan hukum kejahatan dunia maya masih lemah.
Kata Kunci: kejahatan dunia maya, hukum pidana, teknologi informasi

Pendahuluan

Perkembangan masyarakat zaman sekarang ini semakin maju dan di dukung oleh pertumbuhan teknologi telekomunikasi, hingga ikatan antar negara sudah bersifat mendunia sehingga menghasilkan tatanan dunia baru. Demikian ini tidak dapat dipungkiri bahwa dampaknya terhadap perkembangan masyarakat Indonesia yang sedang membangun di era reformasi itu telah dihadapkan dengan berbagai krisis, baik politik, ekonomi, dan sosial budaya, dan ini harus ditangani agar bangsa dan negara Indonesia tetap dipandang keberadaannya di antara bangsa-bangsa di dunia.

Perkembangan teknologi informasi dan komunikasi terus berkembang pesat, kini dimungkinkan untuk menggunakan teknologi informasi dan komunikasi melalui perangkat mobile.Kegiatan yang biasanya dilakukan di dunia nyata kini banyak diperdagangkan melalui gadget (seperti perbankan dan pengiriman surat ke dalam kegiatan dunia maya). perkembangan dari. Transaksi berpindah dengan menggunakan i-Pad, Smartphone, handphone, laptop. Kita tidak lagi mengalami kesulitan untuk mengakses informasi dari seluruh penjuru dunia. Selain banyaknya teknologi informasi dan komunikasi yang telah memberikan dukungan untuk banyak perangkat mobile, juga karena banyak tersedianya hotspot gratis dibanyak tempat. Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah "*cybercrime*".

Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya

mencakup Indonesia, tetapi juga mencakup seluruh dunia. Beberapa kejahatan yang terjadi disebabkan oleh maraknya penggunaan e-mail, e-banking dan e-commerce di Indonesia.

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU Cybercrime (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Penentuan sebagai tindak pidana merupakan kebijakan kriminal, yang menurut Sudarto sebagai usaha yang rasional dari masyarakat untuk menanggulangi kajahatan.[1] Di dalam kebijakan kriminal mencakup kebijakan hukum pidana yang disebut juga sebagai kebijakan penanggulangan kejahatan dengan hukum pidana, karena di samping dengan hukum pidana untuk menanggulangi kejahatan, dapat dengan sarana-sarana non-hukum pidana. Hukum pidana selaku fungsi kontrol sosial digunakan untuk memberantas tindak pidana berbentuk pelanggaran norma terkait penggunaan teknologi informasi yang berpotensi pidana, buat melindungi masyarakat dari bahaya tindak pidana tersebut.

Korupsi tidak mustahil diredakan sekiranya semua pihak turut benar-benar *komited* dalam membasmi. Suatu kejahatan apabila tidak dilakukan pembasmian atau penanggulangan, maka secara kriminologis akan memberikan beberapa dampak buruk, antara lain: (1) meningkatnya kejahatan, baik dari aspek kuantitas maupun kualitas; (2) memunculkan bentuk-bentuk kejahatan baru di luar perhitungan umat manusia, yang bisa saja merupakan

[1] Sudarto, *Hukum dan Hukum Pidana* (Bandung: Alumni, 1981), 158.

derivasi dari "kejahatan konservatif"; dan (3) tidak dapat teridentifikasinya sebuah kejahatan sebagai kejahatan.[2]

Keberhasilan pembangunan suatu negara memerlukan persyaratan ketahanan negara dan dukungan otorisasi masyarakat, yaitu suatu keadaan menghindari gangguan-gangguan dan ancaman-ancaman, termasuk bentuk kejahatan. Seiring dengan kemajuan dan perkembangan ilmu pengetahuan dan teknologi dalam masyarakat, hal ini juga berlaku bagi perkembangan kejahatan. Kejahatan yang dilakukan tidak lagi dengan cara tradisional, namun sudah memanfaatkan dan menggunakan peluang yang disediakan oleh kemudahan instrumen modern dengan peralatan yang canggih. Kejahatan ini merupakan kejahatan baru. Yang dimaksud dengan kejahatan yang berkaitan dengan perkembangan sosial bidang ekonomi dalam masyarakat industri yang pelakunya adalah orang-orang kaya, berilmu, dan terorganisir (termasuk dalam *white collar crime*).

Mobilitas kejahatan yang tinggi tidak hanya terjadi di dalam satu wilayah, tetapi juga antar wilayah, bahkan lintas wilayah dan lintas batas negara. Modus operasinya menggunakan peralatan yang kompleks untuk memanfaatkan sepenuhnya kelemahan sistem hukum dan peluang sistem manajemen. Korban bukan lagi seorang individu, melainkan penyerangan terhadap suatu kelompok masyarakat, bahkan negara, dan kemungkinan korban juga tidak menyadari jikalau dirugikan.[3]

Metode Penelitian

Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundang-undangan terkait *cyber-crime*. Metode pengumpulan data

[2] Nafi' Mubarok, *Kriminologi dalam perspektif Islam* (Sidoarjo: Dwiputra Pustaka Jaya, 2017), 2–3.

[3] Kunarto, "Gelagat Perkembangan Kejahatan dan Kebijakan Penanggulangannya" (Seminar Kriminologi VIII, Semarang: Fakultas Hukum Universitas Diponegoro, 1991), 2.

dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain. Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan *cyber law* di Indonesia.

Pendekatan yang dipergunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Penulis mengkaji Undang-Undang mengenai *cyber law* sedangkan Bahan Hukum yang dipergunakan adalah bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundang-undangan yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.[4]

Batasan Cybercrime

Menurut Widodo, bahwa *cybercrime* diartikan sebagai kegiatan seseorang, sekelompok orang, badan hukum yang memakai komputer bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran (target).

Beberapa tipe kejahatan yang sering terjadi di Internet yaitu:

1. *Illegal acces/unauthorized access to computer system and service*

   Ini adalah bentuk kejahatan yang dilakukan dengan cara meretas/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin dari pemilik sistem jaringan komputer yang dimasukinya.
2. *Illegal contents*

   Memasukkan data atau informasi tentang hal yang tidak benar, tidak etis, serta dapat dianggap melanggar

[4] Soerjono Soekanto dan Sri Marmudji, *Peneltian Hukum Normatif* (Jakarta: Raja Grafindo Persada, 2001), 12–15.

hukum atau mengganggu ketertiban umum kedalam internet, itu adalah suatu modus kejahatan *cybercrime* ini.

3. *Data forgery*

   Ini merupakan modus kriminal di dunia maya yang dilakukan dengan memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. Kejahatan sejenis ini biasanya menargetkan dokumen *e-commerce*, seolah-olah ada "*typo*" yang pada akhirnya akan menguntungkan pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku.[5]

4. *Cyber espionage*

   Ini ialah bentuk kejahatan yang memakai jaringan internet dengan cara memasuki sistem jaringan komputer pihak yang akan ditargetkan menjadi sasaran untuk dimata-matai.

5. *Cyber sabotage and extortion* (sabotase dan pemerasan dunia maya)

   Dalam jenis kejahatan ini, modus biasanya dijalankan dengan mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan *logic bomb*, virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan dan tidak dapat beroperasi secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh penjahat sesuai kebutuhan.

6. *Offense against intellectual property* (pelanggaran terhadap Hak atas Kekayaan Intelektual)

   Modus operandi kejahatan ini adalah menyasar hak kekayaan intelektual yang dimiliki pihak lain di Internet.

[5] Yuni Fitriani dan Roida Pakpahan, "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," *Cakrawala: Jurnal Humaniora* 20, no. 1 (Maret 2020): 22.

Misalnya, meniru tampilan website orang lain secara ilegal.

7. *Infringements of privacy*

   Jenis kejahatan ini rata-rata menargetkan informasi pribadi yang disimpan dalam formulir data pribadi yang tersimpan secara computerized, apabila orang lain mengetahuinya, hal itu dapat menyebabkan kerugian terhadap korban secara *materiil* maupun *immaterial*, seperti bocornya nomor PIN ATM, dan lainnya.

Sifat kejahatan *cybercrime* dapat diklasifikasikan sebagai berikut:[6]

1. *Cyber crime* sebagai tindakan kriminal

   Cyber crime seperti yang dimaksud ialah sebuah tindak kejahatan yang dilakukan dengan konsep kriminalitas yang menggunakan internet sebagai wahana kejahatan. Misalnya *carding*: mencuri kode PIN ATM milik orang lain buat digunakan dalam transaksi online di internet, dan pemanfaatan media internet (*webserver*, *mailing list*) untuk mengedarkan alat-alat pembajakan. Pengirim *e-mail* anonim yang bermuatan iklan (*spamming*) juga dapat dicantumkan dalam contoh kejahatan yang memanfaatkan internet sebagai medianya dan dapat dituntut dengan tuduhan pelanggaran privasi.[7]

2. *Cyber crime* sebagai kejahatan "abu-abu"

   Kejahatan semacam itu di Internet termasuk dalam area "abu-abu". Oleh karena itu, karena motif aktivitasnya terkadang bukan kejahatan, maka sulit untuk menentukan apakah perilaku tersebut merupakan kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah istilah yang digunakan untuk memantau sistem orang lain, dan disalahgunakan dengan mengumpulkan informasi sebanyak mungkin dari sistem.

[6] Fiorida Mathilda, "Cyber Crime dalam Sistem Hukum Indonesia," *Sigma-Mu* 4, no. 2 (September 2012): 36.
[7] Mathilda, 37.

Cybercrime: Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, cybercrime umumnya dianggap sebagai computer crime. The U.S. Department of Justice mendefinisikan kejahatan komputer sebagai: "*…any illegal act requiring knowledge of computer technology for its perpe-tration, investigation, or prosecution*". Organization of European Community Development membagikan definisi lain, yaitu: "*any illegal, un-ethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Hamzah mendefinisikan sebagai "kejahatan di bidang pc secara universal bisa dimaksud bagaikan pemakaian pc secara ilegal".

Dari penafsiran di atas, Wisnubroto mengartikan kejahatan PC bagaikan perbuatan melawan hukum yang dicoba dengan memakai pc bagaikan fasilitas/ perlengkapan PC bagaikan objek, baik buat memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Singkatnya, kejahatan komputer didefinisikan sebagai tindakan ilegal yang dilakukan dengan menggunakan teknologi komputer yang kompleks. Selain itu, sejak kejahatan dilakukan di dunia maya melalui internet, muncul istilah *cybercrime*.

Untuk sebagian besar warga yang terbiasa memakai media teknologi komunikasi, *cybercrime* tidaklah sebutan yang asing. *Cybercrime* ataupun kejahatan dunia maya ialah fenomena yang tidak dapat disangkal. Tidak nampak tetapi nyata. Permasalahan *cybercrime* yang bermacam-macam terus menjadi bertambah tiap harinya, paling utama di negara yang belum terdapat kepastian hukum di bidang teknologi komunikasi modern (*convergence*).

Meskipun mereka tak ingin dipanggil sebagai penjahat karena perbuatannya, namun mereka tidak berbeda dengan penjahat. Karena teknologi komunikasi ini punya kekuatan yang luar biasa untuk mengubah prilaku komunikasi manusia, tehnologi ini selain ada manfaat berwujud kemudahan komunikasi, juga memiliki sisi yang gelap. Salah satu contoh kerugian tehnologi adalah memudahkan para "penjahat" untuk melakukan kejahatan. Penjahat dunia maya

(*cybercrime*) bisa memangsa korbannya, itu adalah kemungkinan dari kemajuan tehnologi itu sendiri.

Raharjo meyakini bahwa kejahatan merupakan fenomena sosial yang sudah ada di dunia mulai awal pada kehidupan manusia. Kejahatan yang lebih maju (modern) adalah suatu bentuk pengubahan kejahatan dari bentuk asli karena tehnologi komunikasi.[8] Wajah kejahatan juga sudah diperhalus dengan sedemikian rupa, kejahatan konvensional di dunia nyata timbul ke dunia maya dengan cara virtual. Pada faktanya, *cybercrime* telah menimbulkan begitu banyak korban dan kerugian moril dan materil. Korban dapat berupa *netizen* (penghuni *cyberspace*) dan masyarakat umum. Namun pada negara berkembang dengan ketimpangan digital seprti Indonesia, tak menganggapnya sebagai bentuk kejahatan.

Seperti halnya kehidupan nyata, ada yang hitam dan ada yang putih, ada yang berperan seperti pahlawan, dan ada pula yang seperti penjahat. Untuk memahami cybercrime, kita juga kudu memahami apa yang disebut dengan hacker, cracker dan lainnya.

Lebih detailnya adalah sebagai berikut:

1. *Hacker*

   Menurut Ustadiyanto definisi *hacker* adalah orang-orang yang ahli dalam bidangnya.[9] *Hacker* ialah orang-orang yang doyan mempelajari komplikasi sistem komputer dan melakukan eksperimen. Mereka cerdas dan mahir untuk menyusup ke dalam jaringan komunikasi suatu pranata di dunia maya. Peretas ini anti sensor, anti penipuan, dan memaksakan hasrat orang lain. Mereka bertaut prinsip bahwa *hacker* bermaksud meningkatkan keamanan jaringan internet. Mereka memuliakan etika atau norma yang berlangsung di dunia maya.

[8] Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi* (Bandung: Citra Aditya Bakti, 02), 29.
[9] Riyeke Ustadiyanto, *Framework e-Commerce* (Yogyakarta: Andi, 2001), 304.

Contohnya, jika ada sebuah perusahaan perbankkan mengatakan tentang jaringan sistem komunikasinya sangat rumit dan mustahil untuk diretas serta tak akan ada yang berhasil menembus. Maka *hacker* akan menghadapi tantangan tersebut, dan selepas berhasil mereka akan memperingatkan alangkah lemahnya sistem informasi perusahaan itu. Oleh karena itu, tak sedikit dari mereka yang berakhir dengan direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

2. *Cracker*

   Di dunia maya, ada beberapa sisi menakutkan dari *hacker*. Mereka disebut *cracker*. Para *cracker* secara ilegal menyusup, menembus, serta merusak situs web, dan sistem keamanan jaringan internet hanya untuk tujuan hiburan dan keuntungan. Setelah berhasil menghancurkan situs sebuah perusahaan, mereka merasa bangga. Serangan *cracer* juga sangat luar biasa. Ada sekitar 100 serangan *cracker* dalam sehari. Info tersebut diperoleh dari Kementerian Pertahanan Amerika Serikat di Pentagon.

3. *Carder*

   Carder merupakan orang yang melakukan *cracking*, ialah pembobolan kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk keuntungan pribadi. Umumnya yang menjadi korban adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil penelitian kejahatan *carding*, pada tahun 2002 Indonesia menduduki peringkat kedua setelah Ukraina.

4. *Deface*

   Deface merupakan suatu gerakan menyusup ke suatu situs, kemudian mengganti tampilan halaman situs untuk maksud tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. Tampilan homepage Polri juga diubah menjadi gambar wanita telanjang.

5. *Phreaker*

   Merupakan seseorang yang melaksanakan *cracking* yang berkenaan dengan jaringan telepon, sehingga dapat melakukan panggilan secara gratis kemana saja. Di Indonesia, kasus seperti ini pernah terjadi pada beberapa warung telepon.

Para karakter *hacker* biasanya tak berasal dari kaum bawah, mereka biasanya ialah orang-orang terpelajar, yang setidaknya mengenyam pendidikan sampai tingkat tertentu dan bisa menggunakan ataupun mengoperasikan komputer. Para craker juga termasuk orang yang berpendidikan, tidak buta teknologi, mampu menurut finansial, serta tidak termasuk dalam masyarakat kelas bawah. Kejahatan seperti ini dapat diklasifikasikan sebagai "*white collar crime*" (kejahatan kerah putih). Jo Ann L. Miller, membagi pelakunya menjadi 4 (empat) kategori:[10]

1. *Organizational occupational crime*

   Penjahat melakukan tindakan ilegal atau merugikan orang lain lewat jaringan internet buat kepentingan atau keuntungan suatu perusahaan. Pelaku biasanya adalah para eksekutif.

2. *Government occupational crime*

   Melakukan suatu tindakan yang ilegal melalui internet, namun dengan persetujuan atau perintah dari negara (pemerintah), Pelakunya sendiri ialah pejabat (birokrat) meski dalam banyak kasus bilamana hal tersebut terkuak, maka akan dibantah.

3. *Professional occupational crime*

   Beragam pekerjaan yang melakukan kejahatan secara disengaja (malpraktik).

4. *Individual occupational crime*

   Ialah para pengusaha, pemilik modal atau orang-orang independen lainnya yang melakukan perbuatan menyimpang, walaupun tingkat sosial ekonominya mungkin tidak tinggi. Dalam aspek pekerjaannya,

[10] M. E. Fuady, "Fenomena Kejahatan Melalui Internet di Indonesia," *Mediator* 6, no. 2 (Desember 2005): 258.

kelompok ini mengambil jalan yang menyimpang dan melanggar hukum atau merugikan orang lain.

Dibandingkan dengan kejahatan konvensional, *cybercrime* memiliki karakteristik yang unik yaitu :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang atau dunia maya, sehingga tidak mungkin untuk menentukan yurisdiksi hukum negara mana yang berlaku untuk tindakan tersebut.
2. Perbuatan tersebut dilakukan dengan menggunakan (perangkat) apapun yang dapat tersambung ke internet.
3. Kerugian material maupun non-material yang disebabkan oleh tindakan-tindakan ini seringkali lebih besar daripada kejahatan tradisional.
4. Pelakunya ialah orang yang dapat menguasai penggunaan internet dan aplikasinya.
5. Perbuatan tersebut acapkali dilakukan secara transnasional.

Cybercrime di Indonesia

Di antara negara berkembang, Indonesia merupakan salah satu negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia kurang memprioritaskan pengembangan teknologi dan penguasaan strategi. Yang terjadi saat itu adalah transfer teknologi dari negara maju tidak otomatis dikuasai oleh negara berkembang seperti Indonesia. Sungguh ironis, karena pada sekitar tahun 1980 Indonesia merupakan negara Asia Tenggara yang memiliki satelit komunikasi pertama kali. Namun sekarang Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, sudah menjadi negara maju berbasis teknologi komunikasi modern.[11]

Walaupun masih ada kontroversi, bisa dikatakan bahwa Indonesia ialah negara dengan kesenjangan digital yang cukup besar. Kesenjangan digital bisa dijelaskan sebagai adanya kesenjangan antara mereka yang bisa menggunakan

[11] Fuady, 258.

teknologi komunikasi dan mereka yang tidak bisa. Selain kesenjangan tingkat pendidikan dan ekonomi di Indonesia, akses teknologi komunikasi Indonesia juga belum merata. Ketimpangan, kurangnya informasi dan telekomunikasi dapat dibagi menjadi beberapa kategori. Tentunya yang paling banyak dikunjungi adalah yang paling dekat dengan pusat informasi komunitas (masyarakat).

Terlepas dari kesenjangan digital, kejahatan dunia maya (*cybercrime*) di Indonesia masih merajalela. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para hacker hitam. Mereka dapat menggunakan kartu kredit orang lain untuk mendapatkan apa pun yang mereka butuhkan, mulai dari berlian, radar laut, *corporate software*, computer server, Harley Davidson, hingga senjata M-16.

Kejahatan tersebut biasa disebut dengan (*credit card fraud*) atau *carding*. Indradi memaparkan,[12] *carding* ialah penipuan terhadap kartu kredit apabila pelaku mengerti nomor kartu kredit seseorang yang masih berlaku, kemudian pelaku dapat membeli perlengkapan secara online dan mengirimkan tagihan kepada pemilik asli kartu kredit tersebut, pelaku carding biasa disebut *carder*. Dalam kejahatan ini, pemilik kartu kredit akan kehilangan uangnya karena orang lain menggunakannya untuk berbelanja dengan mencuri rekening kartu kreditnya. Pencurian akun ini bisa dilakukan dengan cara membobol keamanan toko online tempat pembelian dilakukan. Apalagi jika keamanan toko online tersebut tidak kuat, maka akun kartu kredit yang kemungkinan dibajak oleh para pelaku *carding* (*carder*) akan bertambah.

Berdasarkan kasus dan keadaan cybercrime yang berlangsung di Indonesia, bisa terlihat bahwa *cybercrime* melahirkan ancaman serius bagi departemen keamanan non tradisional. Di Indonesia, kejahatan cyber crime merupakan salah satu kejahatan tertinggi di dunia. Istilah keamanan disebut sebagai kemampuan negara untuk mendeskripsikan

[12] Ade Arie Sam Indradi, *Carding: Modus Operandi, Penyidikan dan Penindakan* (Jakarta: Grafika Indah, 2006), 36.

konsep ancaman dengan mengedepankan aspek militer dalam penyelesaiannya.

Seperti yang dikatakan oleh Walt, penelitian keamanan adalah fenomena perang yang ditegaskan sebagai, "*the study of threat, use, and control of military force*".[13] Namun, setelah tuntasnya perang dingin, makna dari istilah keamanan mengalami perubahan, keamanan meliputi sudut-sudut yang lebih luas, semacam masalah lingkungan hidup, hak asasi manusia, ekonomi, sosial masyarakat, budaya, dan sebagainya. Perubahan makna dan konsep keamanan ini disebabkan oleh berbagai perkembangan, seperti tren global. Revolusi di bidang teknologi komunikasi menunjukkan salah satu tren perkembangan, perubahan ini memungkinkan jarak dapat dihilangkan dan didukung oleh fasilitas transportasi dunia yang semakin kompleks. Situasi ini akan berdampak pada perkembangan problematis masalah politik global, termasuk masalah keamanan.

Pengaturan *Cyber Crime* dalam sistem Hukum Pidana Indonesia

Sistem hukum Indonesia tidak secara spesifik mengontrol tentang hukum siber, namun beberapa undang-undang telah mengatur pencegahan kejahatan siber, seperti Undang-undang No. 36 tentang 1999 tentang Telekomunikasi, Undang-undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang dan peraturan tersebut ini telah mengkriminalisasi jenis[14] kejahatan dunia maya (*cybercrime*) dan ancaman hukuman buat setiap pelanggarnya.

---

[13] Barry Buzan, *People, State, And Fear : A Agenda For Internasional Security Studies in The Post Cold Era*, 2nd edition (London: Harvester Whatsheaf, 1991), 187.

[14] Thantawi, "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia," *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala* 2, no. 1 (Februari 2014): 37.

Selain itu, kebijakan kriminalisasi yang tertulis dalam golongan *cyber crime* telah dirumuskan dalam RKUHP yang terdapat pada Buku Kedua (Bab VIII): Tindak Pidana yang membahayakan keamanan Umum bagi Orang, Barang, Lingkungan Hidup. Bagian Kelima: Pasal 373- 379 tentang Tindak Pidana terhadap Informatika dan Telematika, yang mengatur tindak pidana *illegal access*, *illegal interception*, *data interference* dan *system interference*, penyalahgunaan nama domain, dan pornografi anak.

Dalam pembahasan perkembangan hukum pidana yang akan datang, penyelesaian dan pencegahan *cybercrime* kudu diimbangi dengan penertiban dan pengembangan seluruh sistem hukum pidana, yang mencakup pembangunan struktur, budaya, serta substansi hukum pidana. Dalam kondisi demikian, kebijakan hukum pidana menempati letak yang strategis dalam perkembangan hukum pidana modern. Kebijakan hukum pidana berniat untuk mencapai kedamaian dan kesejahteraan semua orang.

Berikut tindakan kejahatan dunia maya (*cybercrime*) yang di atur dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang No. 19 Tahun 2016 tentang Perubahan atas Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagai berikut:

1. Tindakan yang melanggar kesusilaan.

   Pada Pasal 27 ayat (1) Undang-undang No. 11 Tahun 2008 disebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak membagikan atau menyebarkan atau membuat dapat diaksesnya Informasi Elektronik atau Dokumen Elektronik yang memiliki isi yang melanggar kesusilaan". Namun perbuatan membagikan/ menyebarkan/membuat konten informasi elektronik/dokumen elektronik yang melanggar kesopanan (kesusilaan) tidak dijelaskan dengan sendirinya dalam Undang-undang No. 11 Tahun 2008. Pelanggaran etika/kesusilaan melalui media internet sendiri merujuk pada KUHP.

Dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, dalam Pasal 27 ayat (1) Undang-undang Nomor 11 Tahun 2008 mengatur tentang informasi dan transaksi elektronik, termasuk pornografi *online* dan prostitusi *online*. Jika kejahatan ini dilakukan terhadap anak-anak, maka akan menjadi semakin serius. Salah satu permasalahan yang diakibatkan oleh perkembangan teknologi informasi melalui jaringan internet adalah banyaknya situs yang menampilkan adegan porno. Tampaknya saat ini, sangat sulit melindungi Internet dari gangguan pedagang hiburan yang menjual pornografi.[15]

2. Perjudian

   Perjudian online diatur pada Pasal 27 ayat (2) Undang-undang Informasi dan Transaksi Elektronik. Dalam peraturan ini juga sama disebutkan bahwa: "Setiap orang dengan sengaja dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan perjudian".

3. Penghinaan atau pencemaran nama baik

   Pencemaran nama baik ataupun penghinaan di dunia maya merupakan larangan yang diatur pada Pasal 27 ayat (3) Undang-undang No. 11 Tahun 2008, yang berbunyi : "Setiap Orang dengan sengaja, dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan penghinaan atau pencemaran nama baik." Pembuat undang-undang menyamakan antara penghinaan dan pencemaran. Penghinaan sendiri ialah sebuah perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran

   Pembuat undang-undang sendiri kelihatannya mau mengarahkan perbuatan penghinaan dari media internet tersebut sebagai pencemaran. Dalam Bab XVI Buku II

[15] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Bandung: Refika Aditama, 2005), 146.

mengatur tentang perbuatan penghinaan dan pencemaran. Kejahatan penghinaan terdiri dari penghinaan umum dan penghinaan khusus. Penghinaan umum mengacu pada obyek harga diri dan derajat orang pribadi, termasuk juga pencemaran. Sedangkan penghinaan khusus mengacu pada penghinaan yang memiliki obyek harga diri, kehormatan dan nama baik terbuka (umum). [16] Tindakan penghinaan ataupun pencemaran dapat ditemukan di berbagai kolom komentar di dunia maya, terutama ketika korban memindai identitas, foto, atau video pribadinya. Pelaku juga dapat menulis teks yang menghina atau memfitnah di dinding pernyataan untuk membuat pernyataan atau menghubungkan pernyataan tersebut dengan korban.

4. Pemerasan atau pengancaman

   Pada Pasal 27 ayat (4) Undang-undang No. 11 Tahun 2008 melarang pemerasan atau pengancaman di dunia maya. Dalam pasal tersebut dijelaskan: "Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman".

   Pasal 368 (1) KUHP mencantumkan kualifikasi perbuatan yang terhitung pemerasan atau pengancaman, yaitu: "Setiap orang yang bermaksud untuk menguntungkan dirinya sendiri atau orang lain secara melawan hukum (ilegal), memaksa seseorang untuk memberikan sesuatu milik orang tersebut maupun orang lain secara keseluruhan maupun sebagian dengan kekerasan maupun ancaman kekerasan atau menciptakan hutang maupun menghapus hutang, akan dihukum karena pemerasan dan dapat dijatuhi hukuman hingga 9 tahun penjara."

5. Penguntitan (*cyberstalking*)

[16] Adami Chazawi, *Hukum Pidana Positif Penghinaan*, Edisi Revisi (Malang: Media Nusa Creative, 2013), 81.

Undang-undang No. 11 Tahun 2008 Pasal 29 mengatur bahwa: "Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi". Ketentuan mengenai informasi dan transaksi elektronik dalam Pasal 29 mengatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan ketakutan, termasuk kata-kata atau tindakan tertentu. Ketentuan tersebut serupa dengan pengaturan *cyberstalking* di Amerika Serikat, Kanada, Inggis dan negara lainnya. Tindakan ini dilakukan dengan memanfaatkan teknologi informasi dan komukasi, semisal dengan *mail bombs, unsolicited hate mail*, *obsence or threatening email*, dan yang lainnya.[17]

6. Penyebaran berita palsu (*hoax*)

   Penyebaran berita palsu diatur dalam Undang-undang No. 11/2008 Pasal 28 ayat (1), berbunyi : "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong/palsu serta menyesatkan, yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

7. Ujaran kebencian

   Pasal 28 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentang pidana tersebut, yang berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang dirancang untuk menimbulkan kebencian atau permusuhan individu/ kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA)".

8. Akses ilegal

   Undang-undang No. 11 Tahun 2008, dalam Pasal 30 mengatur sebagai berikut:

[17] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: Refika Aditama, 2012), 177–78.

a. Siapapun yang dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik orang lain dengan cara apapun.
b. Siapapun dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses (membuka) Komputer atau Sistem Elektronik dengan cara apapun dengan maksud untuk memperoleh Informasi Elektronik atau Dokumen Elektronik.
c. Siapapun yang melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik."

Pencegahan dan Penanggulangan Cybercrime

Tindak pidana cybercrime memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Kebanyakan dari korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka saat ini, dan yang perlu dilakukan sekarang adalah mencegah kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan tersebut dapat berupa:[18]

1. *Educate user* (memberikan pengetahuan baru tentang *Cyber Crime* dan dunia internet)
2. *Use hacker's perspective* (menggunakan pemikiran hacker untuk melindungi sistem anda)
3. *Patch system* (menutup lubang-lubang kelemahan pada sistem)
4. *Policy* (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5. *IDS* (Intrusion Detection System) *bundled with IPS* (Intrusion Prevention System)
6. *Firewall*.
7. *AntiVirus*.

[18] Dista Amalia Arifah, "Kasus Cybercrime di Indonesia," *Jurnal Bisnis dan Ekonomi (JBE)* 18, no. 2 (September 2011): 189.

Beberapa langkah penting yang harus diambil dalam menanggapi Cybercrime adalah :

1. Melakukan pembaruan hukum pidana nasional dan hukum acara, sesuai dengan kesepakatan internasional yang terkait dengan kejahatan tersebut.
2. Meningkatkan sistem keamanan jaringan komputer nasional sesuai dengan standar internasional.
3. Meningkatkan pengetahuan dan keahlian aparat penegak hukum dalam upaya pencegahan, investigasi, dan penuntutan kasus-kasus yang berkaitan dengan *cybercrime*.
4. Meningkatkan kesadaran warga negara tentang masalah *cybercrime* dan pentingnya mencegah kejahatan itu terjadi.
5. Meningkatkan kerjasama dari berbagai negara, baik kerja sama bilateral, regional maupun multilateral dalam upaya mengatasi *cybercrime*, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik (mutual assistance treaties).

Beberapa contoh dari bentuk penanggulangan yang lain yaitu:

1. IDCERT (*Indonesia Computer Emergency Response Team*)

   Salah satu cara untuk membuat masalah keamanan lebih mudah ditangani adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Dengan munculnya "*sendmail worm*" (sekitar tahun 1988), masalah keamanan semacam ini mulai dikenali di luar negeri, ketika worm menutup sistem email Internet era itu. Selepasnya dibentuk sebuah (CERT) Computer Emergency Response Team, sejak itu di negara lain juga mulai membentuk CERT untuk dijadikan *point of contact* guna orang untuk mengadukan problem kemanan. IDCERT merupakan CERT Indonesia.[19]
2. Sertifikasi perangkat security

   Peralatan yang dipakai guna membereskan keamanan harus memiliki tingkat karakteristik. Tentunya peralatan

[19] Arifah, 190.

yang digunakan untuk tujuan pribadi berbeda dengan yang digunakan untuk tujuan militer. Tetapi sejauh ini di Indonesia belum ada institusi yang menangani problem evaluasi perangkat keamanan.

Penegakan Hukum terhadap Pelaku Tindak Pidana *Cyber Crime* di Indonesia

Masih terdapat kendala dalam tindakan penegakan hukum terhadap pelaku cybercrime meskipun Undang-undang ITE telah disahkan menjadi Undang-undang No. 11 Tahun 2008 yang menyangkut Informasi dan Transaksi Elektronik. Isi dalam Pasal 5 Seputar perluasan alat bukti baru sesuai dengan hukum acara yang berlaku di Indonesia, menerima informasi elektronik dan data elektronik atau hasil cetak sebagai alat bukti yang sah. Undang-Undang tersebut menambah fakta *cybercrime* yang sebelumnya tidak diatur dalam Kitab Undang-undang Hukum Acara Pidana (KUHAP) seperti isi dalam pasal itu.

Penegakan hukum terhadap pelaku kejahatan siber masih terkendala oleh beberapa aspek, yaitu: aparat penegak hukum kurang memiliki keterampilan atau kualitas dalam menumpasas para cracker dunia maya, keterbatasan alat (media) serta perlengkapan terbaru yang dimiliki Kepolisian. Seperti alat yang seharusnya ada disetiap Polda berfungsi mempercepat deteksi dan prediksi keberadaan para cracker saat beraksi yaitu laboratorium cyber crime. Namun hanya Mabes Polri dan Kepolisian di beberapa Kota Besar yang memiliki Laboratorium itu, sehingga terdapat hambatan ketelatan dan anggaran tinggi dalam setiap proses penyelidikan pekara cybercrime di Indonesia, serta para korban yang enggan mengadukan kejahatan yang menerpa dirinya karena dalih privasi, ekonomi, maupun korban tidak mempercayai keahlian dan pengabdian polisi dalam mengungkap kasus tersebut.[20]

[20] Thantawi, "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia," 38.

Perlindungan Hukum terhadap Korban Tindak Pidana *Cyber Crime* dalam Sistem Hukum Pidana Indonesia

Tindakan penegak hukum terhadap pelaku tindak pidana dunia maya adalah untuk melindungi pengguna cyberspace dari para cracker yang menggunakan media internet dalam melakukan kejahatannya. Meskipun Indonesia belum memiliki "*cyberlaw*" yang secara khusus menargetkan kepentingan korban, namun Indonesia tetap perlu tindakan hukum dengan menggunakan hukum yang ada sebelumnya seperti: perundang-undangan, yurisprudensi maupun konvensi-konvensi Internasional yang sudah diratifikasi untuk melindungi kepentingan penduduk dunia maya di Indonesia

Berbagai upaya dapat diambil untuk menyelesaikan kejahatan Internet, baik secara premetif, preventif, maupun represif. Upaya premetif dapat dijalankan dengan meratifikasi kesepakatan *cyber crime* internasional kedalam sistem hukum di Indonesia. Kesepakatan Dewan Eropa ialah salah satu wujud kesepakatan internasional, dan sebagian kovenannya telah diratifikasi kedalam sistem perundang-undangan di Indonesia. Penanggulangan *cyber crime* secara preventif dapat dijalankan dengan cara mengembangkan pengamanan, meningkatkan energi guna fitur komputer, kemampuan dan kedisplinan dalam memakai fitur tersebut di dunia maya. Aktifitas tersebut bisa berbentuk aksi yang dapat dijalankan baik secara individu, kebijakan nasional, ataupun global. Sementara itu tindakan penanggulangan *cybercrime* secara represif dapat dilaksanakan dengan menjerat para pelaku tindak pidana untuk ditangani sesuai dengan undang-undang. Undang-undang menentukan kepentingan korban dengan memberikan restitusi, kompensasi, ataupun asistensi yang merupakan tanggung jawab pelaku dengan Negara sebagai penyedianya.[21]

Upaya untuk melindungi korban tindak pidana merupakan usaha untuk memulihkan kerugian yang sudah di dapat oleh korban. Perihal ini bakal lebih masuk akal jika

[21] Thantawi, 39.

korban terlibat atau ikut serta dalam proses penyelesaian kasus pidana. Penegakan hukum adalah upaya pembangunan berkelanjutan yang bertujuan untuk mewujudkan kehidupan yang aman, tentram, tertib, dan dinamis bagi negara dan lingkungan negara dalam lingkungan pergaulan dunia yang merdeka (independen).[22]

Dimasa mendatang, penegakan hukum pidana hendaknya lebih memperhatikan kepada sistem keadilan restoratif, ini merupakan solusi yang adil untuk mengaitkan pelaku, korban, keluarganya, serta pihak lain yang terlibat dalam tindak pidana untuk bersama-sama berupaya menyelesaikan tindak pidana tersebut. Hal itu berdasarkan surat keputusan bersama antara Pimpinan Mahkamah Agung RI, Menteri Hukum dan Hak Asasi Manusia (HAM), Menteri Sosial, dan Menteri Pemberdayaan Perempuan dan Perlindungan Anak RI, yang menekankan pemulihan ke keadaan semula.

Hambatan dalam Penanganan Cybercrime

Sekalipun telah ada sebagian pasal yang dapat menjebloskan para pelaku kejahatan *cyber* ke penjara. Namun masih terdapat kendala-kendala dalam penerapannya di lapangan, di antaranya sebagai berikut:

1. Perangkat hukum yang belum memadai

   Terhadap pasal-pasal yang ada dalam KUHP, para penyidik (terutama Polri) menganalogikan (mengumpamakan) dan mempersamakan, serta sepikiran bahwa kudu dibuat Undang-Undang yang khusus mengelola *cybercrime*.
2. Kemampuan penyidik

   Secara umum, pengetahuan dan pemahaman pengoperasian komputer penyidik Polri terhadap hacker komputer, serta kemampuan menyelidiki kasus-kasus tersebut masih sangat minim.

Beberapa faktor yang sangat berpengaruh (determinan) adalah:

[22] Thantawi, 39.

1. Kurangnya pengetahuan tentang komputer

   Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas.
2. Faktor sistem pembuktian yang menyulitkan para penyidik, antara lain:
   a. Alat bukti

      Permasalahan yang dihadapi di dalam penyidikan terhadap *cybercrime* menyangkut persoalan alat bukti, antara lain bertautan dengan ciri kejahatan *cybercrime* itu sendiri, ialah: target ataupun media *cybercrime* merupakan informasi ataupun sistem pc (sistem internet) yang dapat dengan gampang diganti, dihapus ataupun dirahasiakan oleh pelaku kejahatan. *Cybercrime* biasanya dilangsungkan dengan sedikit saksi. Kebalikannya, saksi korban kerapkali terletak jauh di luar negara sehingga menyulitkan penyidik untuk melaksanakan pengecekan saksi serta pengajuan hasil investigasi.
   b. Fasilitas komputer forensik

      Guna menunjukkan jejak para hacker serta cracker ketika melakukan aksinya, terpenting yang berkaitan dengan program serta informasi pc, fasilitas yang dimiliki Polri kurang mencukupi sebab tidak adanya komputr forensik. Sarana ini dibutuhkan guna menampilkan informasi digital dan merekam serta menaruh fakta dalam bentuk soft copy (gambar, program, dan lain-lain.). Dalam kasus ini Polri masih belum memiliki sarana forensic computing yang memadai. Sarana perhitungan forensik yang hendak dibangun oleh kepolisian diharapkan bisa memberikan tiga layanan penting, meliputi : pengumpulan barang bukti (*evidence collection*), *forensic analysis*, dan *expert witness*.[23]

[23] Arifah, "Kasus Cybercrime di Indonesia," 193.

Penutup

Widodo mengatakan bahwa, *cybercrime* diartikan sebagai kegiatan seseorang, sekelompok orang, Badan Hukum yang memakai komputer bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran (target). Dalam pengertian lain Wisnubroto mengartikan kejahatan komputer sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan komputer sebagai sarana/alat komputer sebagai objek, baik untuk mendapatkan keuntungan maupun tidak, dengan merugikan pihak lain.

Sifat kejahatan cybercrime dapat diklasifikasikan menjadi :

1. *Cyber crime* sebagai tindakan kriminal.
2. *Cyber crime* sebagai kejahatan "abu-abu".

Teknologi komunikasi memiliki kekuatan yang luar biasa dalam mengubah perilaku komunikasi manusia, selain membawa manfaat berupa kemudahan komunikasi, teknologi juga dapat membawa kerugian, salah satunya memudahkan para "penjahat" untuk melakukan kejahatan. Kemajuan teknologi memungkinkan penjahat dunia maya (*cybercrime*) memangsa korbannya. Beberapa kejahatan *cybercrime* yang umum terjadi adalah *hacker*, *cracker*, *carding*, *deface*, dan *phreaker*. Para pelaku hacker biasanya bukan berasal dari kaum bawah, mereka umumnya merupakan orang-orang terpelajar, yang paling tidak mengenyam pembelajaran resmi hingga tingkatan tertentu serta bisa memakai ataupun mengoperasikan pc. Para *craker* pula merupakan orang yang berpendidikan, tidak buta teknologi, sanggup secara finansial, serta tidak tercantum dalam warga kelas dasar.

Berdasarkan kasus dan kondisi *cybercrime* yang terjadi di Indonesia, dapat terlihat bahwa *cybercrime* merupakan ancaman serius bagi departemen keamanan non tradisional. Di Indonesia, kejahatan penggunaan perangkat komputer dan internet (*cybercrime*) merupakan salah satu kejahatan tertinggi di dunia. Sistem hukum Indonesia tidak secara spesifik mengatur tentang hukum siber (*cybercrime*),

namun beberapa undang-undang telah mengatur pencegahan kejahatan siber, seperti Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi, Undang-undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam pembahasan perkembangan hukum pidana dimasa mendatang, penanggulangan dan pencegahan *cybercrime* kudu diimbangi dengan pembenahan serta pengembangan seluruh sistem hukum pidana, yang meliputi pembangunan struktur, budaya, serta substansi hukum pidana. Dalam kondisi demikian, kebijakan hukum pidana menempati posisi yang strategis dalam kemajuan hukum pidana modern. Serta penegakan hukum pidana hendaknya lebih memperhatikan kepada sistem keadilan restoratif (*Restorative Justice*), sepertinya ini merupakan solusi yang adil untuk mengaitkan pelaku, korban, keluarganya, serta pihak lain yang terlibat dalam tindak pidana untuk bersama-sama berupaya menyelesaikan tindak pidana tersebut.

Daftar Pustaka

Arifah, Dista Amalia. "Kasus Cybercrime di Indonesia." *Jurnal Bisnis dan Ekonomi (JBE)* 18, no. 2 (September 2011).

Buzan, Barry. *People, State, And Fear : A Agenda For Internasional Security Studies in The Post Cold Era*. 2nd edition. London: Harvester Whatsheaf, 1991.

Chazawi, Adami. *Hukum Pidana Positif Penghinaan*. Edisi Revisi. Malang: Media Nusa Creative, 2013.

Fitriani, Yuni, dan Roida Pakpahan. "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace." *Cakrawala: Jurnal Humaniora* 20, no. 1 (Maret 2020).

Fuady, M. E. "Fenomena Kejahatan Melalui Internet di Indonesia." *Mediator* 6, no. 2 (Desember 2005).

Indradi, Ade Arie Sam. *Carding: Modus Operandi, Penyidikan dan Penindakan*. Jakarta: Grafika Indah, 2006.

Kunarto. "Gelagat Perkembangan Kejahatan dan Kebijakan Penanggulangannya." Semarang: Fakultas Hukum Universitas Diponegoro, 1991.

Mathilda, Fiorida. "Cyber Crime dalam Sistem Hukum Indonesia." *Sigma-Mu* 4, no. 2 (September 2012).

Mubarok, Nafi'. *Kriminologi dalam perspektif Islam*. Sidoarjo: Dwiputra Pustaka Jaya, 2017.

Raharjo, Agus. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti, 02.

Soekanto, Soerjono, dan Sri Marmudji. *Peneltian Hukum Normatif*. Jakarta: Raja Grafindo Persada, 2001.

Sudarto. *Hukum dan Hukum Pidana*. Bandung: Alumni, 1981.

Suseno, Sigid. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2012.

Thantawi. "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia." *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala* 2, no. 1 (Februari 2014).

Ustadiyanto, Riyeke. *Framework e-Commerce*. Yogyakarta: Andi, 2001.

Wahid, Abdul, dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2005.