Siyasah: Jurnal Hukum Tata Negara
Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1

Konstruksi Hukum dalam *Cybercrime* Pelaku Kejahatan Teknologi Informasi

Windi Riani[1], Firmansyah[2], Isna Rahmadian[3]

Institut Agama Islam Negeri Metro[123]

windiriyani48@gmail.com[1], firmansipmh@gmail.com[2], isnarahmadian@gmail.com[3]

Article Info

Article history:

Received
29 November 2023
Revised
2 Januari 2024
Accepted 5
Januari 2024

ABSTRACT

Cybercrime develops alongside technological advances, bringing forth both positive and negative impacts. Positive effects include the evolution of social media, email, and internet banking. However, crimes like data hacking have also surfaced, particularly within the banking system, involving the use of specialized tools on ATMs to replicate customer data. This research utilizes normative methods to scrutinize pertinent legal aspects, concentrating on written laws and legislative approaches that govern information and technology. The data were analyzed descriptively by gathering legal materials from relevant literature and regulations. The findings underscore the necessity for formal government intervention, exemplified by the Ministry of Communication and Information, in blocking numbers exploited by fraudsters. Social approaches have been proposed as an alternative to mitigate the risks associated with this crime. Hence, the prevention of cybercrime demands governmental involvement and a comprehensive social approach.

.

Keyword: Cybercrime, Law, Information Technology

Keywords:

Cybercrime, Hukum, Teknologi Informasi

Abstrak

Kejahatan maya atau cybercrime berkembang seiring dengan kemajuan teknologi, menghadirkan dampak positif dan negatif. Dampak positif mencakup perkembangan media sosial, e-mail, dan internet banking. Namun, kejahatan seperti peretasan data (hacking) juga muncul, terutama dalam sistem perbankan dengan penggunaan alat khusus pada ATM untuk menduplikat data nasabah. Penelitian ini menggunakan metode normatif untuk mengkaji aspek hukum terkait, dengan fokus pada hukum tertulis dan pendekatan perundang-undangan yang mengatur informasi dan teknologi. Data dianalisis secara deskriptif melalui pengumpulan bahan hukum dari literatur dan regulasi terkait. Hasilnya menunjukkan perlunya tindakan formal pemerintah, seperti Kementerian Komunikasi dan Informasi, dalam pemblokiran nomor yang digunakan oleh pelaku penipuan. Pendekatan sosial juga diusulkan sebagai alternatif untuk mengurangi risiko kejahatan ini. Oleh karena itu, pencegahan cybercrime memerlukan peran pemerintah dan pendekatan sosial yang holistik.

Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1

Pendahuluan

Perkembangan telekomunikasi dan teknologi informasi saat ini sangat berkembang pesat karena permintaan dan kebutuhan teknologi yang semakin meningkat. Dalam telekomunikasi melahirkan sebuah teknologi yang dikenal dengan sebutan internet. Internet ini meruakan suatu kumpulan jaringan pada perangkat pintar yang dikenal sebagai *gadget* secara global yang saling berhubungan. Sistem pada jaringan komputer yang saling terhubung dengan menggunakan sistem global *Transmission Control Protocol/ Internet Protocol Suite* (TCP/IP) sebagai pertukaran paket (*Packet Switching Communication Protocol*) untuk melayani miliaran pengguna di seluruh dunia. [1]

Cyber Law merupakan aspek hukum yang ruang lingkupnya mencakup dengan hubungan perorangan atau subyek hukum yang menggunakan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia *cyber* atau maya. *Cyber Law* memiliki kata lain yaitu *Cyberspace Law*. Cyeber law memiliki tujuan untuk memenuhi keinginan para pengguna transaksi secara online. Dinamika globalisasi informasi pada elektronik saat ini memerlukan adanya suatu aturan melindungi kepentingan para netter dalam mengakses informasi di dunia maya. [2]

Cyebercrime adalah suatu bentuk kejahatan virtual yang menggunakan media perangkat yang telah terhubung ke internet, perangkat yang digunakan tidak hanya pada computer atau laptop saja, akan tetapi terkadang pada smartphone jga dapat dilakukan kejahatan secara virtual dengan syarat memakai jaringan internet. *Cyebercrime* memiliki definisi yaitu sebagai suatu

[1] Muhammad Khairul Faridi, "KONSTRUKSI HUKUM DALAM PENANGANAN CYBERCRIME" (n.d.): 3.
[2] Sumiaty Adelina Hutabarat et al., *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0* (PT. Sonpedia Publishing Indonesia, 2023), 58.

perbuatan yang melanggar hukum lalu memanfaatkan teknologi computer yang berbasis kecanggihan untuk perkembangan teknologi[3]Kejahatan maya

(*cybercrime*) terjadi disebabkan larna adanya pekembangan pada teknologi, kejahatan tersebut telah mengakibatkan dampak dampak negatif dan positif dari adanya teknologi tersebut. Dampak positif dari adanya teknologi bukan hanya lewat media social akan tetapi perkembangan e-mail, internet banking, serta hal-hal lain. Akan tetapi tidak hanya pada dampak positif saja, dalam perkembangan teknologi ini juga menimbukan dampak negative, peretasan criminal untuk mendapatkan data atau informasi dengan cara meretas (hacking).[4] Pelaku kejahatan ini biasanya orang-orang yang pernah bekerja di bidang perbankan dan menggunakan alat khusus yang dipasang di ATM yang dapat menduplikat data nasabah, sehingga pelaku dapat mengambil uang nasabah tanpa diketahui dengan duplikat data tersebut.

Sehubungan dengan penjelasan di atas, dapat disimpulkan bahwa tindakan kriminal tersebut dapat menimbulkan berbagai masalah dan keresahan di masyarakat, baik secara pribadi maupun bagi banyak orang. Karena perkembangan teknologi informasi pada, UndangUndang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dibuat di Indonesia. Secara umum, undang-undang ITE terdiri dari dua bagian besar yaitu undang-undang yang mengatur transaksi dan informasi elektronik dan undang-undang yang mengatur perbuatan yang dilarang. Selain itu, UU ITE mengatur alat bukti yang diatur dalam KUHAP dan tindakan kejahatan yang diatur dalam KUHP.

[3] Dr Muhammad Ridha Albaar M.Kom S. Kom, *ETIKA PROFESI INFORMATIKA* (uwais inspirasi indonesia, n.d.), 26.
[4] I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha, "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)," *Jurnal Konstruksi Hukum* 1, no. 2 (October 28, 2020): 335.

Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1

Metode Penelitian

Penelitian ini menggunalan metode normative yang mengkaji hukum tertulis dari berbagai segi dan aspek pendekatan perundang-undangan yang memuat norma hukum yang mengikat secara konseptual yang terdapat di masyarakat. Sumber hukum yang akan digunakan bersumber dari penelitian kepustakaan berupa bahan hukum primer berdasarkan Peraturan Perundang-undangan mengenai informasi dan teknologi. Serta berbagai literatur yang mendukung dalam penelitian ini. Metode kajian yang digunakan penulis dengan *library research*, yaitu dengan mencari data-data melalui internet dan buku-buku terkait dengan masalah cybercrime, serta beberapa masalah yang terkait dengan hukum di Indonesia. Data yang sudah terkumpul dianalisis menggunakan metode kualitatif. Hasil analisis data kemudian disajikan secara deskriptif.

PEMBAHASAN

KEJAHATAN *CYEBERCRIME*

Perkembangan teknologi informasi yang sangat berdampak besar bagi manusia telah bisa mengubah keserdasan dan pola fikir manusia. Lihat saja misalnya teknologi informasi mampu membuat manusia semakin kreatif, dengan memanfaatkan teknologi informasi yang ada, manusia bisa membuat aplikasi-aplikasi yang bisa mendatangkan uang. Manusia bisa membuat konten-konten kreator. Bahkan dengan perkembangan teknologi informasi seorang bisa menjadi sukses. [5]Tetapi dengan perkembangan zaman yang sanggat siknifikan banyak sekali manusia yang menyalahgunakan informasi teknologi tersebut.

Bagi sebagaian besar masyarakat yang terbiasa menggunakan media teknologi

[5] Dr Oksidelfa Yanto M.H S. H., *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi* (Samudra Biru, 2021), 25.

komunikasi, *cyebercrime* bukanlah istilah yang asing terdengar. *Cyebercrime* atau kejahatan diruang maya adalah fenomena yang menjadi masalah utama dan tidak dapat terhindarkan. Terdapat berbagai kasus *cyebercrime* yang kian hari kian meningkat, terutama dinegara-negara yang tidak memiliki kepastian hukum dalam bidag teknologi informasi moderen. Teknologi komunikasi yang memiliki kekuatan dasyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki sisi gelapnya tersendiri. Teknologi membawa kerugian, salah satunya berupa semakin

dipermudahkanya penjahat dalam melakukan kejahatanya. Kecanggihan teknologi mempermudah para *cyber* memangsa para korbannya.[6]

Tindak kejahatan ini perlu pengawasan yang sangat ketat baik dari warga Masyarakat maupun para orang tua juga harus mengawasi anak-anak karena kejahatan ini sangat berbeda dengan kejahatan konvensional lainnya. Secara garis besar ada beberapa modus *cybercrime* berdasarkan beberapa isu menurut Mustari dikenal dengan kejahatan kerah biru dan kejahatan kerah putih. *Cybercrime* memiliki karakteristik yaitu:

a) Ruang lingkup kejahatan
b) Sifat kejahatan
c) Pelaku kejahatan
d) Modus kejahatan
e) Jenis kerugian yang ditimbulkan

Berdasarkan karakteristik diatas, Cybercrime diklasifikasikan menjadi:[7]

[6] Muhammad E. Fuady, "'Cybercrime': Fenomena Kejahatan melalui Internet di Indonesia," *Mediator: Jurnal Komunikasi* 6, no. 2 (December 19, 2005): 256.

[7] Lita Sari Marita, "CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA" (n.d.): 4–5.

a) Teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.

b) *Cybertresspass*, yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau indifidu.

c) *Cybervandalism*, yaitu penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data dikomputer Beberapa macam jenis-jenis kejahatan yang sering terjadi di Internet atau dunia maya dintaranya yaitu:[8]

a) *Illegal acces/Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem komputer dan jasa), , Adalah suatu bentuk kejahatan yang dilakukan dengan cara merentas atau memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin atau tanpa sepengetahuan dari si pemilik sistem jaringan komputer yang dimasukinya

b) *Illegal Contents*. Merupakan bentuk kejahatan cybercrime yang melibatkan penyebaran informasi palsu, tidak etis, atau melanggar hukum melalui internet, yang dapat dianggap merugikan atau mengganggu ketertiban umum.

c) *Data Forgery,* Merupakan modus kejahatan di dunia digital yang melibatkan pemalsuan data pada dokumen-dokumen penting yang disimpan sebagai scripless document melalui internet. Umumnya, kejahatan ini ditargetkan pada dokumen-dokumen e-commerce dengan membuat kesan "kesalahan pengetikan," yang pada akhirnya memberikan keuntungan kepada pelaku. Korban cenderung memasukkan informasi pribadi dan nomor kartu kredit, yang kemungkinan besar akan disalahgunakan oleh pelaku kejahatan.

[8] Yuni Fitriani, Roida Pakpahan, "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," *Cakrawala - Jurnal Humaniora* 19, no. 2 (n.d.): 22.

d) *Cyber Espionage (Spionase Cyber).* Adalah suatu kejahatan yang modusnya menggunakan jaringan internet, untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer (computer network system) pihak yang menjadi sasarannya.

e) *Cyber Sabotage and Extortion* (*Sabotase* dan Pemerasan Dunia Maya). Dalam kejahatan ini, modus yang umumnya digunakan melibatkan gangguan, perusakan, atau penghancuran terhadap data, program komputer, atau sistem jaringan komputer yang terkoneksi dengan internet. Kejahatan ini seringkali dilakukan dengan menyisipkan logic bomb, virus komputer, atau program khusus, sehingga mengakibatkan data, program komputer, atau sistem jaringan komputer menjadi tidak dapat digunakan tidak berjalan sebagaimana mestinya atau berjalan namun telah dikendalikan sesuai yang diinginkan oleh si pelaku.

f) *Offense Against Intellectual Property* (Pelanggaran Terhadap Hak atas Kekayaan Intelektual). Kejahatan ini modus operandinya ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai suatu contoh: peniruan tampilan pada suatu web page situs milik orang lain secara illegal.

g) *Infringements of Privacy (Infringements privasi)*. Modus dalam kejahatan ini umumnya berfokus pada akses terhadap informasi pribadi seseorang yang disimpan dalam formulir data pribadi yang terkomputerisasi. Jika informasi ini diketahui oleh pihak lain, dapat menyebabkan kerugian pada korban baik secara materiil maupun immateriil, seperti kebocoran nomor kartu kredit, nomor PIN ATM, dan hal-hal sejenis.

Hacker biasanya tidak berasal dari kaum bawah, mereka biasanya orang-orang terpelajar yang telah belajar setidaknya sedikit dan mahir menggunakan dan mengoperasikan komputer. Mereka juga termasuk orang yang berpendidikan, mampu secara finansial, dan tidak berasal dari masyarakat kelas bawah.

1. KEBIJAKAN HUKUM TERHADAP *CYEBERCRIME*

Sistem hukum Indonesia tidak secara spesifik mengontrol tentang hukum siber, namun ada beberapa undang-undang telah mengatur pencegahan kejahatan siber berikut ini 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 kejahatan dunia maya (*cybercrime*) dan ancaman hukuman buat setiap pelanggarnya.[9]

Sangat penting untuk memiliki peraturan yang mengatur kegiatan manusia yang berkaitan dengan penggunaan teknologi informasi karena masyarakat sedang berubah dan berkembang pesat karena globalisasi dan teknologi, khususnya teknologi informasi. Ditetapkan pada 21 April 2008, UU ITE adalah undang-undang *cyber* pertama di Indonesia yang bertujuan untuk memberikan perlindungan hukum bagi masyarakat yang melakukan transaksi elektronik, mencegah kejahatan berbasis teknologi informasi, dan melindungi masyarakat pengguna jasa yang menggunakan teknologi informasi dan komunikasi. UU tersebut terdiri dari 54 pasal dan dibagi menjadi 13 bab.

Ketentuan rumusan yang mengatur rumusan terkait kriminalisasi perbuatan yang dikategorisasikan sebagai tindak pidana siber terdapat dalam Bab VII tentang Perbuatan yang Dilarang Pasal 27 sampai Pasal 37 beserta sanksi pidananya dalam Bab XI tentang Ketentuan Pidana Pasal 45 sampai Pasal 52. Pasal 1 angka (1) UU ITE mendefinisikan informasi elektronik sebagai data elektronik, termasuk tetapi tidak terbatas

[9] Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (December 19, 2020): 413.

pada tulisan, suara, gambar, peta, rancangan, foto electronic data interchange (EDI), surat elektronik, telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah dan memiliki arti atau dapat dipahami oleh individu yang berkompeten untuk memahaminya. Sementara itu, Pasal 1 angka (4) menjelaskan bahwa dokumen elektronik mencakup segala informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya. Dokumen elektronik dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas

pada tulisan, suara, gambar, peta, rancangan, foto, atau elemen sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang memiliki makna atau dapat dimengerti oleh individu yang memiliki kemampuan untuk memahaminya. [10] Dalam KUHP dapat ditentukan mengenai tindak pidana yang terkait dengan teknologi informasi bisa disebutkan, antara lain:[11]

a) Pasal 362 KUHP untuk kasus *Carding*, yang pelakunya mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di internet untuk melakukan transaksi di *E-Commerce*.
b) Pasal 378 KUHP untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.

[10] Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, and Femmy Silaswaty Faried, "UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA" 3, no. 2 (2020): 282.

[11] Supanto -, "PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY," *Yustisia Jurnal Hukum* 5, no. 1 (April 1, 2016): 57, accessed October 30, 2023, https://jurnal.uns.ac.id/yustisia/article/view/8718.

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

d) Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan e-mail kepada temanteman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* secara berantai melalui *mailling list (millis)* tentang berita yang tidak benar.

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

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

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

Selain itu, kebijakan kriminalisasi yang tercantum dalam kategori cybercrime telah dirumuskan dalam RKUHP, yang terdapat dalam Buku Kedua (Bab VIII) dengan judul "Tindak Pidana yang Mengancam Keamanan Umum untuk Orang, Barang, Lingkungan Hidup." Bagian Kelima dari bab ini, yaitu Pasal 373-379, secara khusus mengatur tindak pidana terkait Informatika dan Telematika. Pasal-pasal tersebut mencakup pelanggaran-pelanggaran seperti illegal access, illegal interception, data interference dan system interference, penyalahgunaan nama domain, dan pornografi anak.

Hacking, atau peretasan, termasuk dalam kategori akses ilegal, seperti yang telah ditunjukkan sebelumnya. Tindak pidana siber yang merusak kerahasiaan, integritas, ketersediaan sistem elektronik, informasi, dan dokumen elektronik berasal dari tindak pidana akses ilegal. Secara umum, ilegal adalah tindakan yang dilakukan seseorang dengan

Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1

sengaja dan tidak memiliki hak untuk mengakses sistem komputer secara keseluruhan atau sebagian. Pengaturan akses ilegal mencakup pelanggaran terhadap keamanan sistem dan data komputer (*integritas*, ketersediaan, dan kerahasiaan), seperti *hacking*, c*racking*, atau komputer *trespass*. Dalam pasal 30 memang sesuai untuk menjerat perbuatan pidana peretasan atau Hacking. Karena tindakan meretas itu termasuk dalam kategori *Illegal Access*. Bagaimana yang disebutkan bahwa:

a) Pasal (30) ayat (1) delik umum akses illegal. Ayat pertama dari pasal ini mengatur Illegal Acces sebagai delik pokok bahwa padasarnya tindakan termasuk komputer atau sistem elektronik tanpa persetujuan pihak yang berhak adalah perbuatan yang dilarang. Perlindungan hukum yang hendak diberikan melalui pasal ini ialah perlindungan terhadap property dan privasi seseorang.
b) Pasal 30 ayat (2) tentang akses illegal mendapatkan informasi. Pasal ini merupakan delik yang kualifisir dari ayat sebelumnya dalam ayat ini ditambahkan unsur unsur tujuan mengakses yaitu untuk memperoleh informasi atau dokumen elektronik. pengaturan ini penting mengingat dalam sistem elektronik yang sifatnya pribadi, rahasia, atau ekonomis
c) Pasal 30 ayat (3) tentang akses illegal dengan melanggar menerobos, melampaui, atau menjebol pengamanan.

Dengan adanya sanksi yang sudah diterangkan di atas maka pelaku kejahatan cyebercrime bisa ditangkap sesuai dengan kesalahan yang dilakukan dengan hukuman yang beraku dalam undang-undang. Sebelum melakukan tindak pidana pasti dilakukannya aspek hukum dalam pembuktian. Dalam konteks hukum, bukti yang digunakan untuk membuktikan suatu tindak pidana harus mematuhi ketentuan undang-undang, sebagaimana dijelaskan dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana. Pentingnya bukti yang sah menjadi landasan, dan keyakinan hakim terhadap bukti-bukti

tersebut menjadi dasar pengambilan keputusan. Berikut beberapa alat bukti yang diatur dalam Pasal 184 Kitab Undang-undang Hukum Acara Pidana sebagai acuan dalam pembuktian kejahatan mayantara *(cybercrime)*, yaitu:[12]

a) Keterangan Saksi

Dalam ranah hukum, pembuktian suatu tindak pidana harus tunduk pada ketentuan undang-undang, sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana. Validitas bukti menjadi aspek krusial, dan keyakinan hakim atas keandalan bukti-bukti tersebut menjadi pijakan utama dalam proses pengambilan keputusan. Keteragan Ahli. Pasal 186 Kitab Undang-Undang Hukum Acara Pidana mengatur persyaratan formal untuk keterangan ahli, yang didefinisikan sebagai pernyataan yang diucapkan oleh seorang ahli dalam sidang pengadilan. Keterangan ahli menjadi sangat relevan terutama ketika jaksa menggunakan bukti elektronik untuk membuktikan keterlibatan pelaku kejahatan dunia maya. Fungsi keterangan ahli dalam konteks ini adalah memberikan klarifikasi di pengadilan bahwa dokumen atau data elektronik yang diajukan merupakan bukti yang sah dan dapat dipertanggungjawabkan secara hukum.

b) Alat bukti surat (Pasal 184 huruf c dan Pasal 187 Kitab Undang-undang Hukum Acara Pidana)

Alat bukti yang diakui berdasarkan jenis surat didasarkan pada Pasal 187 Kitab Undang-Undang Hukum Acara Pidana, terutama surat yang dibuat di atas sumpah jabatan atau dikuatkan dengan sumpah. Dalam konteks cybercrime, surat telah mengalami transformasi dari bentuk tertulis menjadi bentuk tidak tertulis dan

[12] Dwi Nurahman, "KEBIJAKAN PENEGAKAN HUKUM CYBERCRIME DAN PEMBUKTIAN YURIDIS DALAM SISTEM HUKUM PIDANA NASIONAL" 17, no. 2 (n.d.): 149–150.

bersifat online. Terdapat dua kategori alat bukti dalam komputer yang telah disertifikasi. Pertama, hasil cetak dari sistem komputer yang telah mendapatkan sertifikasi dari lembaga berwenang dapat dianggap otentik, contohnya seperti struk yang dikeluarkan oleh bank dalam transaksi ATM. Kedua, sertifikasi dari lembaga yang berwenang dapat dianggap sebagai bukti surat karena dikeluarkan oleh pejabat yang memiliki kewenangan. Jenis alat bukti surat lainnya mencakup bukti elektronik yang dapat dicetak atau dihasilkan dalam bentuk print out, serta surat yang terlihat pada layar monitor dalam jaringan komputer.

c) Alat bukti petunjuk (Pasal 184 (1) huruf d dan Pasal 188 Kitab Undang-undang Hukum Acara Pidana)

Dalam kasus cybercrime, mengumpulkan bukti fisik menjadi tugas yang sulit dilakukan. Salah satu pendekatan yang lebih memungkinkan adalah mencari petunjuk-petunjuk yang menunjukkan adanya niat jahat, seperti akses yang tidak sah. Ini dapat mencakup pemeriksaan keterangan saksi di pengadilan, analisis surat elektronik, hasil cetakan data, atau pernyataan terdakwa di ruang sidang. Pendekatan ini menjadi cara yang lebih praktis dalam mengumpulkan bukti terkait kejahatan dunia maya.

d) Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 Kitab Undang-undang Hukum Acara Pidana)

Keterangan terdakwa merujuk pada apa yang diucapkan oleh terdakwa di pengadilan terkait perbuatannya atau pengetahuannya sendiri. Untuk memastikan keabsahan keterangan terdakwa, syarat formilnya adalah keterangan tersebut harus diucapkan di pengadilan, dan secara materiil, keterangan tersebut harus berkaitan dengan perbuatan yang dilakukan, diketahui, atau dialami oleh terdakwa sendiri.

Siyasah: Jurnal Hukum Tata Negara
Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1

1. PENCEGAHAN KEJAHATAN TERHADAP *CYEBERCRIME*

Dalam rangka penanggulangan kejahatan termasuk penanggulangan kejahatan *cyber* dapat dilakukan melalui 2 (dua) upaya yaitu upaya preventif dan upaya represif. indakan preventif dalam kejahatan merupakan tindakan yang mengharapkan sesuatu itu dapat ditanggulang dan dicegah sebelum kejahatan itu terjadi dalam hal yang lain menharapkan terjadinya penurunan dari kejahatan tersebut atau kejahatan tersebut dapat dihilangkan. Tujuan dari tindakan prevetif seperti pencegahan ini tidak lain tidak bukan seperti yang tertulis dalam Tugas dan wewenang Polri terulis di dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia. Tujuan system peradilan pidana adalah penanggulan kejahatan termasuk dalam kejahatan elektronik . selain dengan hukuman yang sudah dijelaskan dalam undang-undang, pencegahan cyeber juga bisa dilakukan dalam berbagai cara, diantaranya:[13]

a) Patroli *Cyeber*

Patroli *Cyber* adalah patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya patroli siber bertujuaan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial, patroli siber sendiri biasanya dilakukan pada aplikasi seperti instagram, whatsapp, twitter. Patroli siber dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan.

b) Edukasi Cyeber

Edukasi *cyber* sendiri pada dasarnya adalah sebuah pengenalaan akan *cybercrime* dan bahayanya. Edukasi siber lebih lagi ditujukan untuk

[13] Andreas Agung, Hafrida Hafrida, and Erwin Erwin, "Pencegahan Kejahatan Terhadap Cybercrime," *PAMPAS: Journal of Criminal Law* 3, no. 2 (May 11, 2023): 219.

memberikan manfaat informasi tentang *cybercrime* keseluruhan baik, bahayanya, jenis-jenisnya, modusnya serta hukuman akan kejahatan tersebut.

c) Teguran Langsung

Teguran langsung merupakan bentuk lanjutan dari patroli *cyber* teguran langsung diharapkan untuk membuat peringatan akan pelanggaran yang dilakukan oleh masyarakat pada media sosial ataupun internet. Teguran langsung yang dilakukan sendiri biasanya bekerja sama dengan Kemenkominfo untuk melakukan tindakan pencegahan hal-hal yang mendapat teguran berupak konten yang bersifat provokasi, sara, ataupun pornografi.

d) *Teke Down*

Take down merupakan salah satu strategi dari lima bentuk pencegahan yang dilakukan dalam mencegah *cybercrime*, *take down* sendiri jika dijelaskan adalah suatu tindakan untuk menghentikan ataupun menghapus ketersediaan sesuatu yang berada dalam ruang internet seperti video, website, berita ataupun aplikasi yang kurang baik, seperti melanggar etika, moral dan kesopanan serta hukum.

e) Penegakan Hukum

Penegakan hukum merupakan salah satu bentuk pencegahan, tindakan represif sendiri diperlukan untuk memberi efek jera. Penegakan hukum dilakukan pihak aparat kepolisisan sebagai upaya terakhir dalam tindakan pencegahan pidana.

Dalam Upaya pengurangan resiko yang di timbulkan oleh tindak kejahatan penipuan, perlu adanya *absence of capable guardian* oleh pemerintahan sebagai

peran formal. Alam hal ini pihak pemerintah yang menjadi focus utama Seharusnya pihak Pemerintah seperti Kementerian Komunikasi dan Informasi melakuakan pemblokiran terhadap nomor-nomor yang digunakan para pelaku untuk menipu korbanya. [14] Langkah- langlah tersebut lah yang seharusnya menjadi penentu mencegah kemunculan angka-angka yang dimanfaatkan dalam tindak penipuan menunjukkan perlunya pendekatan sosial sebagai cara alternatif untuk mengatasi masalah ini. Upaya pencegahan kejahatan dapat dilakukan melalui pendekatan sosial, di mana suatu lembaga bertanggung jawab untuk menyosialisasikan potensi risiko kejahatan serta memberikan solusi untuk mengurangi kemungkinan terjadinya penipuan. Adopsi langkah-langkah ini dianggap sangat penting guna mengatasi tantangan penipuan yang semakin meresahkan.

Salah satu upaya pencegahan dan pemecahan masalah yang dilakukan oleh pemerintah Kementerian Komunikasi dan Informatika adalah dengan meningkatkan kesadaran masyarakat terhadap kemungkinan terjadinya penipuan mengatasnamakan perusahaan. Pemerintah harus melakukan lebih banyak daripada hanya memberi peringatan kepada pengguna sebagai bentuk kewaspadaan. seperti menginstruksikan pengguna untuk menghindari mempercayai orang yang tidak dikenal, menghindari memberikan kode OTP, dan berhati-hati saat menerima informasi.

Dalam BSSN (Badan Siber dan Sandi Negara) memiliki arah kebijakan dan strategi nasional untuk mengatasi isu-isu strategis dalam menjaga stabilitas

[14] Reza Hikmatulloh and Evy Nurmiati, "Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)," *Kosmik Hukum* 20, no. 2 (July 22, 2020): 126.

keamanan nasional di ruang siber adalah penguatan keamanan dan ketahanan siber yang diwujudkan dengan strategi berikut:[15]

a) Penguatan pengamanan infrastruktur siber.
b) Pembangunan dan penguatan *Computer Emergency Response Team* (CERT).
c) Pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber.
d) Penguatan kapasitas sumber daya manusia keamanan siber.
e) Penyelesaian kejahatan siber *clearance rate* tindak pidana siber. Strategi diatas merupakan implementasi yang mana strategi tersebut akan diterapkan. Negara Indonesia saat ini masi berada pada tahap pembuatan standarisasi

Nasional *Cyber Security* sehingga untuk mencapai *cyber security* yang ideal masi banyak proses yang perlu di lalui memerlukan waktu. Melalui strategi ini diharapkan BSSN sebagai leading sector mampu mengoptimalkan peranannya guna mewujudkan *cyber security* yang ideal bagi Indonesia.

KESIMPULAN

Kecanggihan yang terjadi di dunia teknologi informasi, membuat banyak sekali pihak yang merasakan dampaknya. Kasus yang setiap harinya selalu meningkat dengan kasus cyebercrime yang berbeda beda. Modus yang terjadi pada masalah cyebercrime bermacammacam, seperti seperti kebocoran nomor kartu kredit, nomor PIN ATM, dan hal-hal

[15] Yusep Ginanjar, "STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA," *Jurnal Dinamika Global* 7, no. 02 (December 15, 2022): 302–303.

sejenis. Bahkan dalam kejahatan tersebut sering terdengar di telingga kita, karena kejahatan cyebercrime.

Peraturan Hukum menjadi penyelamat adanya kejahatan cyebercrime, karena di Indonesia sudah banyak peraturan Perundang-undangan yang mengatur tentang kejahatan di dunia teknologi informasi. Dengan menerapkan sanksi serta tindak pidana yang sudah tertulis dalam Kitab Undang-Undang. Adanya sanksi tersebut yang dilakukan oleh pelaku kejahatan cyebercrime untuk memberikan efek jera bagi pelaku, serta tidak akan mengulangi perbuatanya kembali. Upaya pencegahan yang dilakukan agar terhindar dari kejahatan cyebercrime salah satunya yaitu menghindari memberikan kode OTP dan berhati-hati saat menerima informasi. Dan salah satu cara untuk mencegah kejahatan adalah dengan menggunakan pendekatan sosial, di mana suatu lembaga bertanggung jawab untuk mensosialisasikan potensi risiko kejahatan dan menyediakan solusi untuk mengurangi kemungkinan penipuan.

DAFTAR PUSTAKA

-, Supanto. "PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY." *Yustisia Jurnal Hukum* 5, no. 1 (April 1, 2016). Accessed October 30, 2023. https://jurnal.uns.ac.id/yustisia/article/view/8718.

Agung, Andreas, Hafrida Hafrida, and Erwin Erwin. "Pencegahan Kejahatan Terhadap Cybercrime." *PAMPAS: Journal of Criminal Law* 3, no. 2 (May 11, 2023): 212–222.

Faridi, Muhammad Khairul. "KONSTRUKSI HUKUM DALAM PENANGANAN CYBERCRIME" (n.d.).

Fuady, Muhammad E. "'Cybercrime': Fenomena Kejahatan melalui Internet di Indonesia." *Mediator: Jurnal Komunikasi* 6, no. 2 (December 19, 2005): 255–264.

Ginanjar, Yusep. "STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA." *Jurnal Dinamika Global* 7, no. 02 (December 15, 2022): 291–312.

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (December 19, 2020): 400–426.

Hikmatulloh, Reza, and Evy Nurmiati. "Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)." *Kosmik Hukum* 20, no. 2 (July 22, 2020): 121.

Hutabarat, Sumiaty Adelina, Selvia Junita Praja, Didik Suhariyanto, Saptaning Ruju Paminto, Dora Kusumastuti, Rahma Melisha Fajrina, Immi Ira Monalisa Saragih, Eko Budihartono, and Muhamad Abas. *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. PT. Sonpedia Publishing Indonesia, 2023.

Marita, Lita Sari. "CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA" (n.d.).

M.H, Dr Oksidelfa Yanto, S. H. *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi*. Samudra Biru, 2021.

M.Kom, Dr Muhammad Ridha Albaar, S. Kom. *ETIKA PROFESI INFORMATIKA*. uwais inspirasi indonesia, n.d.

Nurahman, Dwi. "KEBIJAKAN PENEGAKAN HUKUM CYBERCRIME DAN PEMBUKTIAN YURIDIS DALAM SISTEM HUKUM PIDANA NASIONAL" 17, no. 2 (n.d.).

Roida Pakpahan, Yuni Fitriani. "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace." *Cakrawala - Jurnal Humaniora* 19, no. 2 (n.d.).

Setiyawan, Wahyu Beny Mukti, Erifendi Churniawan, and Femmy Silaswaty Faried. "UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA" 3, no. 2 (2020).

Singgi, I Gusti Ayu Suanti Karnadi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha. "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* 1, no. 2 (October 28, 2020): 334–339.

Siyasah: Jurnal Hukum Tata Negara
Vol. 03, No. 2, December 2023, pp. 220-239
E-ISSN: 2988-5299, DOI: 10.32332/siyasah.v4i1