Jurnal Hukum dan Sosial Politik
Vol.1, No.2 Mei 2023
e-ISSN: 2986-3287; p-ISSN: 2986-4445, Hal 60-67

Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime

Musa Sahat Tobing[1], Utari Wulandari[2], Marito Sari Sihotang[3], Raihana[4]
[1,2,3]Universitas Lancang Kuning
[4]Universitas Muhammadiyah Riau

Abstract*. When surfing the digital world, you need to be careful about feeling comfortable on social media. Cybercrime is a form of crime that arises because of the use of internet technology. In line with advances in information technology, several crimes have emerged which are often interpreted as crimes committed in cyber space or areas. Rusbagio Ishak, Kadit Serse Polda Central Java said, this cyber crime has the potential to cause losses in several fields: political, economic, socio-cultural. Cyber crime is various kinds of illegal access to a data transmission. In other words, cybercrime is an illegal activity on a computer system or is included in the category of crimes in cyberspace. The target of this cyber crime is a computer connected to the internet network. Cyber crime is carried out with various purposes. Starting from fun testing hacking skills, to serious crimes that can harm the victim financially. One of the cyber crimes that is rife in Indonesia is a social engineering attack or social engineering. Social engineering is a manipulation technique that exploits human error to gain access to personal information or valuable data..*

Keywords*: Cyber Law, Modes, Digital.*

Abstrak. Ketika berselancar di dunia digital, Anda perlu berhati-hati dengan rasa nyaman di media sosial. Cyber crime merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Sejalan dengan kemajuan teknologi infomasi, telah muncul beberapa kejahatan yang sering dipersesikan sebagai kejahatan yang dilakukan dalam ruang atau wilayah siber. Rusbagio Ishak, Kadit Serse Polda Jateng megatakan, cyber crime ini potensial meimbulkan kerugiann pada beberapa bidang: politik, ekonomi, social budaya. Cyber crime adalah berbagai macam akses ilegal terhadap suatu transmisi data. Dengan kata lain, kejahatan siber merupakan aktivitas yang tidak sah pada suatu sistem komputer atau masuk dalam kategori tindak kejahatan di dunia maya. Sasaran kejahatan siber ini adalah komputer yang terhubung ke jaringan internet. Cyber crime dilakukan dengan beragam tujuan. Mulai dari iseng mengetes kemampuan hacking, hingga kejahatan serius yang bisa merugikan korbannya secara finansial. Salah satu kejahatan siber yang marak terjadi di Indonesia adalah social engineering attack atau rekayasa sosial. Social engineering merupakan teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses informasi pribadi atau data berharga.

Kata kunci: Hukum Cyber, Modus-Modus, Digital.

Received Maret 07, 2023; Revised April 02, 2023; Accepted Mei 12, 2023
* Musa Sahat Tobing

LATAR BELAKANG

Teknologi informasi memegang peranan penting, baik di masa kini maupun di masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang sangat besar bagi negara di dunia. Adapun implikasi dari pertumbuhan teknologi informasi membawa masyarakat kepada pola perilaku yang semakin terbuka.[1] Perkembangan masyarakat era kini merupakan industrialisasi, serta ditopang perkembangan teknologi telekomunikasi, maka hubungan antar negara sudah bersifat mendunia yang kemudian menciptakan dunia tatanan baru.[2] Internet merupakan salah satu aspek yang mengalami perkembangan yang sangat pesat. Internet sudah menjadi salah satu kewajiban dalam hidup saat ini.[3] Fakta tersebut juga mempengaruhi terhadap perkembangan kejahatan. Kasus kejahatan siber di Indonesia sudah banyak terjadi, mulai dari penipuan identitas hingga teror tagihan utang yang bahkan tidak pernah dilakukan. Berbagai kejahatan siber ini pun banyak dilakukan melalui media sosial, seperti Facebook, WhatsApp, Instagram, dan masih banyak lagi. Maka untuk menghadapi hal tersebut, Direktur Cybersecurity BDO in Indonesia dan Co-Founder Indonesia Cyber Security Forum (ICSF) M Novel Ariyadi menjelaskan faktor-faktor utama penyebab terjadinya kejahatan siber yang membedakan dengan kejahatan umumnya. Hal tersebut disampaikannya dalam kegiatan media clinicyang bertema Peran Identitas Digital yang Aman dalam Meningkatkan Kepercayaan pada Fintech, dan dilaksanakan pada Kamis (4/11/2021). Sementara tiga faktor yang menyebabkan kejahatan siber diantaranya adalah:

1. Identitas pengguna

Fitur yang memudahkan manipulasi kelengkapan di media sosial seringkali dimanfaatkan pengguna dengan niat yang tidak baik. Selain itu, data-data pengguna lain juga mudah dicuri. Hal ini kemudian memudahkan pelaku kejahatan siber untuk memanipulasi korban.

---

[1] Nur Khalimatus Sa'diyah, MODUS OPERANDI TINDAK PIDANA CRACKER MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK, PERSPEKTIF
Volume XVII, No. 2 Tahun 2012 Edisi Mei, hlm. 79.

[2] Supanti, "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasi Dengan Penal Policy", *Jurnal Yustisia* Vo. 5, No. 1 Januari-April 2016, hlm. 53.

[3] Alcianno G. Gani, "Cyber Crime (Kejahatan Berbasis Komputer), *Jurnal Sistem Informasi (JIS)*, Vol. 5 No. 1 2018, hlm. 17.

2. Penggandaan aset informasi

Aset informasi yang ada di media sosial juga dapat dengan mudah digandakan oleh pengguna. Hal ini dikarenakan tidak adanya fitur untuk menghapus atau disebut pula 'delete button' di internet.

3. Lokasi

Faktor lainnya yang dapat memicu ancaman serangan kejahatan siber adalah ketika lokasi pengguna dapat dideteksi di media sosial. Sama halnya dengan kemudahan untuk dipalsukan ataupun disembunyikan. Tidak hanya itu, pemerintah sendiri adalah penjamin dan sumber identitas antara orang ke orang lainnya pada ranah offline.

"Hal ini berbeda sekali dengan identitas fisik yang harus melewati banyak sekali proses jika ada yang mau memalsukan identitas, tapi di dunia digital orang bisa hanya dengan beberapa klik dapat merubah identitas," tutur Novel.

Berbeda dengan ranah online, pemerintah harus melakukan kerja sama dengan identity provider untuk dapat menjamin verifikasi identitas dan tanda tangan elektronik. Setidaknya, dalam ranah perlindungan identitas digital dari kejahatan siber, harus ada kerja sama antara pemberi kebijakan, pengelola sistem elektronik, serta pengguna internet pula.

"Tiga aspek perlindungan data pribadi, mulai dari pemerintah, pengguna, hingga pengelola sistem elektronik yang ikut serta bertanggung jawab untuk melindungi identitas digital, yaitu penyelenggara sertifikasi elektronik (PSRE)," pungkas Nove.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur (library research)[4]. Jenis penelitian ini adalah normatif, sehingga sumber data yang digunakan adalah data primer dari peraturan perundang-undangan, data sekunder dari tinjauan Pustaka dan data tersier dari kamus, media dan ensiklopedia. Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur (library research). Jenis pendekatan penelitian yang digunakan oleh peneliti di dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan teori dan asas hukum, terkhususnya dalam penelitian ini difokuskan pada pembahasan mengenai kekuatan-kekuatan sosial yang

[4] P. Andi, *Metode Penelitian Kualitatif Dalam Perspektif Rancangan Penelitian*, Yogyakarta, Ar-Ruzz Media.

mempengaruhi hukum dan fungsi hukum di masyarakat. Penelitian hukum normatif didefinisikan penelitian yang mengacu kepada norma-norma hukum yang terdapat dalam peraturan perundang-undangan maupun putusan pengadilan. Penelitian hukum normatif bisa juga disebut sebagai penelitian hukum doctrinal. Prosedur dalam penelitian ini dilaksanakan dengan tahapan-tahapan yaitu mengumpulkan data pustaka, membaca, mencatat, menelaah, mengumpulkan konsep atau naskah kemudian dilakukan elaborasi dan eksplanasi terhadap data atau teks yang terkumpul berkaitan dengan topik pembahasan utama di dalam penelitian ini. Hal ini sesuai dengan pendapat Zed yang mengatakan bahwa riset pustaka tidak hanya sebatas urusan membaca dan mencatat literatur atau buku, melainkan serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca, mencatat serta mengolah suatu bahan penelitian.

HASIL DAN PEMBAHASAN

Modus-Modus Cyber Crime

Perkembangan teknologi informasi semakin pesat dan meluas sehingga kegiatan sehari-hari semakin tergantung pada penggunaan teknologi digital. Namun, di sisi lain, kejahatan cyber juga semakin meningkat dengan munculnya ragam modus cyber crimeyang semakin kompleks.[5] Cybercrime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.[6] Menurut Widodo, *cyber crime* adalah kegiatan seseorang, sekelompok orang, badan hukum yang memakai computer bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran target.[7] Formulasi kejahatan di dunia maya dapat dilihat pada pengaturan tindakan tersebut dalam undang-undang. Dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur sejumlah perbuatan yang dilarang yang menjadi tindakan

[5] Dede Handayani et.al, RAGAM MODUS CYBER CRIME DI ERA DIGITAL 4.0, Abdi Jurnal Publikasi Vol. 1, No. 4, Maret 2023, hlm. 423.

[6] Lita Sari Marita, CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA,Cakrawala: Jurnal Humaniora Bina Sarana Informatika, 2015.

[7] Miftakhur Rokhman Habibi-Isnatul Liviani, "Kejahatan Teknologi Informasi (*Cyber Crime*) Dan Penanggulangannya Dalam Sistem Hukum Indonesia", *Al-Qaunun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, Vol. 23, No. 2 Desember 2020, hlm. 404.

cybercrime.[8] *Cyber crime* merupakan salah satu tindak pidana. Penentuan sebagai tindak pidana merupakan bagian kebijakan kriminal, yang menurut Sudarto sebagai usaha yang rasional dari masyarakat untuk menanggulangi kejahatan.[9] Berikut penjelasan atas 5 modus cybercrime yang paling banyak terjadi:

Phising

Pelaku biasanya akan mengaku dari lembaga resmi melalui sambungan telepon, email atau pesan teks. Mereka memanipulasi korban supaya mau memberikan data pribadi yang akan digunakan untuk mengakses akun penting milik korban. Phishing bisa mengakibatkan berbagai kerugian, antara lain pencurian identitas pribadi.

Kejahatan Carding

Carding adalah jenis kejahatan dunia maya yang dilakukan dengan bertransaksi menggunakan kartu kredit milik orang lain. Jadi, setelah mengetahui nomor kartu kredit korban, pelaku kemudian berbelanja online dengan kartu kredit curian ituNomor kartu kredit tersebut dicuri dari situs atau website yang tidak aman. Bisa juga diperoleh dengan cara membeli dari jaringan spammer atau pencuri data. Selanjutnya data kartu kredit itu disalahgunakan oleh carder, sebutan pelaku kejahatan carding.

Ransomware adalah malware atau software jahat yang bukan hanya bisa menginfeksi komputer, tapi juga menyandera data pengguna. Tindak kejahatan ini dapat menimbulkan kerugian besar bagi korbannya.

Pelaku akan meminta uang tebusan ke korban jika ingin ransomware dihapus atau dimusnahkan. Apabila korban tidak mengabulkan permintaan tersebut, pelaku tak segan-segan mengancam akan membuat data menjadi korup alias tidak bisa digunakan lagi.

Penipuan online

Penipuan online atau penipuan digital yang saat ini makin banyak modusnya. Di antaranya adalah modus penipuan berkedok foto selfie dengan KTP atau identitas diri.

Foto selfie bersama KTP biasanya menjadi salah satu syarat registrasi online akun keuangan, seperti dompet digital, paylater, pinjaman online, sampai daftar rekening bank online

[8] Dewi Bunga, POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME, 2Jurnal LEGISLASI INDONESIA Vol 16 No.1 - Maret 2019, hlm. 4.
[9] Sudarto, *Hukum Dan Hukum Pidana*, Bandung, Alumni, 1981, hlm. 158.

Bisa saja kamu terjebak aplikasi pinjaman online palsu yang dibuat sedemikian rupa. Kemudian oleh pelaku, data kamu dipakai untuk pencucian uang, dijual di pasar gelap, atau digunakan sesuka hati untuk pinjaman online ilegal.

Cara Mengatasi Modus-Modus Dalam Cyber Crime

Cyber crime meskipun bersifat virtual dapat dikategorikan sebagaitindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruangcyber sudah tidak pada tempatnya lagi untuk kategorikan sesuatu denganukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek danperbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitandanhal-halyanglolosdarijerathukum.[10] Anda harus mengetahui dan mempraktikkan cara mengatasi cyber crime berikut ini bila pernah menjadi korban sehingga kejadian buruk tersebut tidak terulang lagi.

Mengambil Kembali Data-Data yang Sempat Diretas

Peretasan data dan kerugian lainnya yang disebabkan cyber crime pasti membuat Anda panik. Namun, Anda tetap harus berpikir jernih agar tidak mengalami kerugian secara masif. Sebaiknya Anda lekas berupaya mengambil kembali data-data yang sempat diretas. Hubungi tim support IT untuk membantu mengembalikan data-data yang diretas pelaku cyber crime. Bila data-data Anda berhasil diselamatkan, barulah Anda bisa melakukan beberapa cara mengatasi cyber crime lainnya sebagai tindak lanjut.

Menggunakan Gadget untuk Kepentingan Pribadi

Penggunaan dari gadget memiliki dampak positif maupun negatif dalam kehidupan manusia.[11] Penggunaan gadget yang dilakukan untuk kepentingan bersama memang rentan membuat Anda menjadi korban cyber crime. Karena bukan mustahil bila akun Anda akan disalahgunakan oleh oknum tak bertanggung jawab. Alangkah lebih baik bila Anda menggunakan gadget untuk kebutuhan pribadi. Lindungi gadget dengan username dan password supaya data-data penting Anda tidak bisa diakses sembarang orang.

---

[10] Muhammad Anthony Aldriano dan Mas Agus Priyambodo, CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA, Jurnal Kewarganegaraan Vol. 6 No. 1 Juni 2022, hlm. 2170.

[11] Erga Yuhandra *et.al*, "Penyuluhan Hukum Tentang Dampak Positif Dan Negatif Penggunaan Gadget Dan Media Sosial", *Empowerment : Jurnal Pengabdian Masyarakat*, Vol. 4, No. 1 2021, hlm. 83.

Memprioritaskan Penggunaan Software Asli

Anda tak perlu ragu menyiapkan bujet demi mendapatkan software asli. Karena biasanya software bajakan sudah terkontaminasi malware atau jenis virus lainnya. Meskipun harga software asli lebih mahal, kualitasnya tentu sebanding dengan biaya yang mesti Anda keluarkan. Selain itu, Anda juga bisa mendapatkan update otomatis secara resmi jika menggunakan software asli.

Melakukan Update Software secara Rutin

Jangan mengabaikan manfaat update software secara rutin. Ternyata aktivitas ini merupakan salah satu cara mengatasi cyber crime yang ampuh. Software terbaru biasanya sudah dilengkapi proteksi keamanan yang lebih baik dari versi software sebelumnya. Sehingga penggunaan software versi terbaru akan melindungi data-data Anda dari incaran pelaku cyber crime. Risiko data hilang akibat virus pun semakin kecil kalau Anda rajin melakukan update software.

Mengaktifkan Data Encryption

Manfaat data encryption untuk melindungi data-data penting memang tak boleh dianggap remeh. Anda wajib mengaktifkan data encryption pada jaringan lokal seperti LAN atau nirkabel di rumah dan kantor. Aktivasi data encryption akan mencegah akses yang berstatus tidak sah serta meminimalkan risiko penyadapan teks.

Menggunakan Hosting yang Aman

Anda mesti cermat memilih layanan hosting yang aman ketika memilih website. Biasanya layanan hosting berkualitas dilengkapi sistem proteksi khusus untuk melindungi data dari serangan malware. Perlindungan ini akan membuat data-data website Anda tidak mudah diretas dan disalahgunakan pelaku cyber crime.

KESIMPULAN DAN SARAN

Internet sebenarnya memiliki sisi negatif dalam perkembangannya, karena membuka peluang aktivitas anti sosial yang sebelumnya dianggap tidak mungkin atau tidak mungkin dilakukan. Menurut teori tersebut, kejahatan adalah produk dari masyarakat itu sendiri, yang berarti bahwa masyarakat itu sendiri yang menciptakan kejahatan. Fenomena cybercrime patut diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Cybercrime dapat dilakukan tanpa mengenal batas wilayah dan tidak memerlukan interaksi langsung antara pelaku dan korban kejahatan.

DAFTAR REFERENSI

Alcianno G. Gani, 2018, "Cyber Crime (Kejahatan Berbasis Komputer), *Jurnal Sistem Informasi (JIS)*, Vol. 5 No. 1.

Dede Handayani et.al, 2023, RAGAM MODUS CYBER CRIME DI ERA DIGITAL 4.0, Abdi Jurnal Publikasi Vol. 1, No. 4, Maret.

Dewi Bunga, 2019, POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME, 2Jurnal LEGISLASI INDONESIA Vol 16 No.1 – Maret.

Erga Yuhandra *et.al*, 2021, "Penyuluhan Hukum Tentang Dampak Positif Dan Negatif Penggunaan Gadget Dan Media Sosial", *Empowerment : Jurnal Pengabdian Masyarakat*, Vol. 4, No. 1.

Lita Sari Marita, 2015, CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA,Cakrawala: Jurnal Humaniora Bina Sarana Informatika.

Miftakhur Rokhman Habibi-Isnatul Liviani, 2020, "Kejahatan Teknologi Informasi (*Cyber Crime*) Dan Penanggulangannya Dalam Sistem Hukum Indonesia", *Al-Qaunun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, Vol. 23, No. 2 Desember.

Muhammad Anthony Aldriano dan Mas Agus Priyambodo, 2022, CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA, Jurnal Kewarganegaraan Vol. 6 No. 1 Juni.

Nur Khalimatus Sa'diyah, 2012, MODUS OPERANDI TINDAK PIDANA CRACKER MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK, PERSPEKTIF Volume XVII, No. 2 Mei.

P. Andi, 2012, *Metode Penelitian Kualitatif Dalam Perspektif Rancangan Penelitian*, Yogyakarta, Ar-Ruzz Media.

Sudarto, 1981, *Hukum Dan Hukum Pidana*, Bandung, Alumni.

Supanti, 2016, "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasi Dengan Penal Policy", *Jurnal Yustisia* Vo. 5, No. 1 Januari-April.