MULTIPLE
Journal of Global and Multidisciplinary
https://journal.institercom-edu.org/index.php/multiple
Volume 2 Issue 3 (2024) E-ISSN 2988-7828
INSTITERCOM PUBLISHER

Analisa Yuridis Terhadap Peningkatan Tindak Cyber Crime Ditinjau Dari Perspektif Hukum Pidana

Mohamad Firdaus[1*]
[1]Universitas Indraprasta PGRI, Indonesia
Article Info: Accepted: 16 Maret 2024; Approve: 25 Maret 2024; Published: 30 Maret 2024

Abstrak: Revolusi Industri 4.0 merupakan era industri keempat dengan ditandai munculnya terobosan teknologi disejumlah bidang ketergantungan masyarakat dengan teknologi sudah tidak dapat terelakkan, disatu sisi sangat menguntungkan disegala bidang, namun disisi lain terdapat pemanfaatan untuk melakukan kejahatan melalui dunia maya atau yang kita kenal dengan cyber crime.Dalam penelitian ini diigunakan metode yuridis empiris dengan bahan primer, UUD 1945, KUHP dan UU No 19 Tahun 2016 tentang perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, untuk bahan sekunder diambil dari buku, jurnal, internet, doktrin, artikel dan asas-asas hukum, pendapat hukum juga diperoleh melalui beberapa narasumber.Teknik Pengumpulan data adalah studi Kepustakaan dan wawancara dengan narasumber. Analisis data yang digunakan dalam penelitian ini adalah analisis secara kualitatif. Dengan penelitian ini diperoleh hasil bahwa, cyber crime kejahatan siber di Indonesia dari tahun ke tahunnya meningkat. Dapat dibuktikan dari jumlah serangan siber (Cyber Attack) selama Januari Agustus 2019 sebesar 39.330.231 serangan mejadi 189.937.542 serangan ditahun 2020 selama Januari Agustus sedangkan upaya penanggulangan tindak pidana cyber crime dilakukan, meliputi atas: Sarana Penal (Kebijakan Penal) dan Sarana Non Penal (Kebijakan Non Penal) Sarana dan kebijakan yang ada diharapkan dapat menanggulangi tindak pidana cyber crime, walaupun tidak bisa sepenuhnya bisa mengatasi tindak pidana tersebut. Peningkatan kualitas sarana dan kebijakan dalam menanggulangi kejahatan ini yang sangat dibutuhkan.
Kata Kunci: Analisa Yuridis; Cyber Crime; Perspektif Hukum Pidana.

Abstract: *Industrial Revolution 4.0 is the fourth industrial era marked by the emergence of technological breakthroughs in a number of fields. Society's dependence on technology is inevitable. On the one hand, it is very profitable in all fields, but on the other hand, there is use to commit crimes through cyberspace or what we know as cyber crime. This research used empirical juridical methods with primary materials, the 1945 Constitution, the Criminal Code and Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, secondary materials were taken from books, journals, the internet, doctrine, articles and legal principles, legal opinions were also obtained through several sources. Data collection techniques were literature studies and interviews with sources. The data analysis used in this research is qualitative analysis. With this research, the results obtained are that cyber crime in Indonesia is increasing from year to year. It can be proven from the number of cyber attacks (Cyber Attack) during January August 2019 which was 39,330,231 attacks to 189,937,542 attacks in 2020 during January August while efforts to overcome cyber crime were carried out, including: Penal Facilities (Penal Policy) and Non Facilities Penal (Non-Penal Policy) Existing facilities and policies are expected to be able to overcome cyber crimes, although they cannot completely overcome these criminal acts. Improving the quality of facilities and policies in dealing with this crime is very much needed.*
Keywords: *Juridical Analysis; Cyber Crime; Criminal Law Perspective.*

Correspondence Author: Mohamad Firdaus
Email: mfirdausmumu@gmail.com

Pendahuluan

Revolusi Industri 4.0 merupakan era industri keempat dengan ditandai munculnya terobosan teknologi disejumlah bidang. Bidang-bidang yang dimaksud meliputi bidang robotika, kecerdasan buatan, nanoteknologi komputasi kuantum, bioteknologi. *Industrial Internet of Things*, Teknologi nirkabel generasi kelima (5G), aditif manufaktur/percetakan 3D dan Industri Otomi penuh (Savitri, 2009). Industri-Industri tersebut mengubah tatanan diseluruh dunia tak terkecuali Indonesia.

Pemanfaatan teknologi di era revolusi Industri 4.0 sangat luar biasa, apalagi dimasa pandemi Covid 19 saat ini , semua aktivitas berjalan melalui teknologi digital berupa informasi, media dan komunikasi untuk menanggulangi penyebaran virus covid 19 yang sampai detik ini belum dapat diatasi, perkembangan dan kemajuan teknologi semakin signifikan, ketergantungan masyarakat dengan teknologi sudah tidak dapat terelakkan, disatu sisi sangat menguntungkan disegala bidang, namun disisi lain terdapat pemanfaatan untuk melakukan kejahatan melalui dunia maya atau yang kita kenal dengan *cyber crime* (kejahatan siber).

Selain itu pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum (Suhariyanto, 2012)

Perbuatan melawan hukum merupakan sebuah kejahatan/Tindak Pidana yang melanggar aturan Undang-Undang, fenomena ini merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi informasi sebagaimana dikemukakan oleh Ronni R.Nitisbaskara bahwa (R.Nitisbaskara, 2005) interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Menjawab tuntutan dan tantangan komunikasi global lewat internet, Undang-Undang yang diharapkan (ius konstituendum) adalah perangkat hukum. Yang permasalahannya termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Pada dasarnya teknologi internet merupakan sesuatu yang bersifat netral, dalam artian bahwa teknologi tersebut tidak bersifat baik ataupun jahat. Akan tetapi dengan keluasan fungsi dan kecanggihan teknologi informasi yang terkandung di dalamnya semakin merebaknya globalisasi dalam kehidupan mendorong para pelaku kejahatan untuk menggunakan internet

sebagai sarananya. *cyber crime* (kejahatan siber) pada saatnya akan menjadi bentuk kejahatan serius yang dapat membahayakan keamanan individu, masyarakat dan negara serta tatanan kehidupan global.

Perkembangan teknologi dan globalisasi telah membawa dampak signifikan terhadap munculnya kejahatan baru di era digital. Di Indonesia, seperti di banyak negara lain, kejahatan cyber crime atau kejahatan siber semakin berkembang pesat seiring dengan pesatnya perkembangan teknologi. Beberapa contoh kejahatan cyber crime yang semakin marak dan meningkat meliputi memalsukan akun media sosial seperti Facebook, WhatsApp, Instagram, dan Twitter seseorang, fenomena ransomware WannaCry, pencurian data, cyber terorisme, hacking, carding, defacing, cybersquatting, cyber typosquatting, menyebarkan konten ilegal, dan penyebaran malware. Kejahatan-kejahatan ini memberikan tantangan serius bagi keamanan cyber dan privasi individu serta organisasi. Oleh karena itu, pemerintah dan lembaga terkait perlu mengambil langkah-langkah yang efektif untuk melawan dan mencegah kejahatan-kejahatan siber ini demi melindungi masyarakat dan infrastruktur digital negara. Dengan demikian, tujuan dilakukan penelitian ini adalah untuk mengetahui analisa yuridis terhadap peningkatan tindak cyber crime ditinjau dari perspektif hukum pidana.

Kajian Teori

1. Data Peningkatan Tindak Pidana Cyber Crime (kejahatan siber) Dari Berbagai Sumber di Indonesia

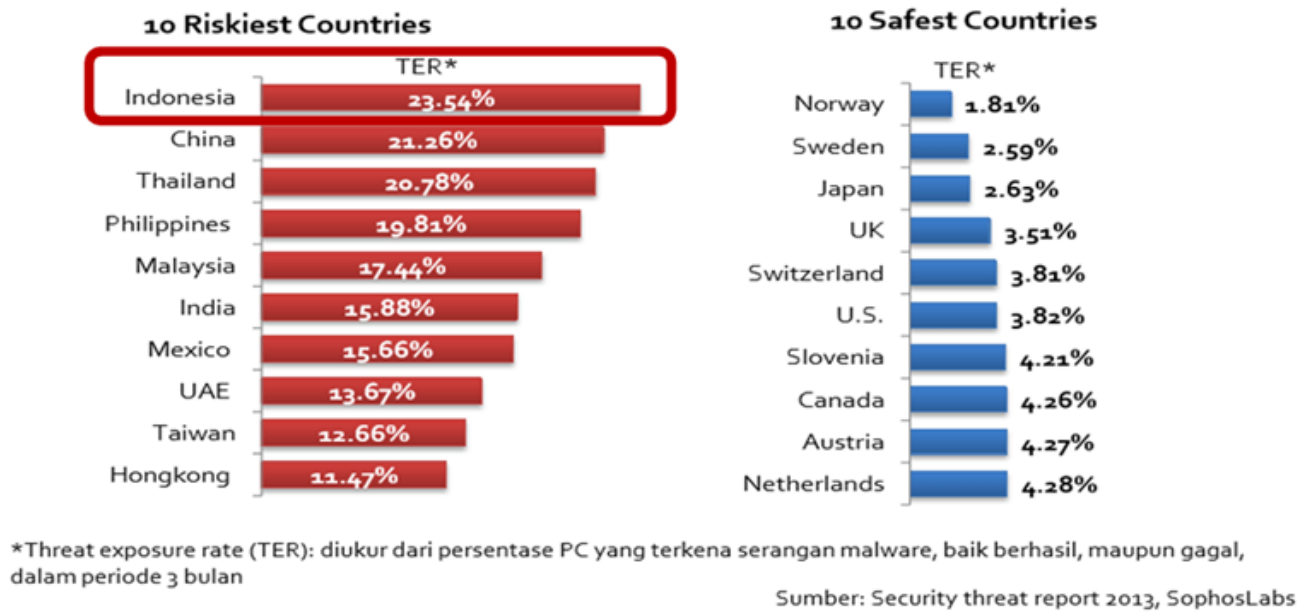
Sebagai negara hukum selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum. Karena hal itu, Indonesia selalu berusaha untuk melakukan pembaharuan Hukum Pidana, salah satunya dengan menerbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)(Pasal 26 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2016). Karena penyelenggaraan kegiatan dalam bidang teknologi yang berbasis komputer sangat penting bagi masyarakat, dan rawan dalam melakukan pelanggaran hak asasi manusia. Instrumen hukum memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan kepada para pelaku *Cyber crime* (kejahatan siber). Sebagai hukum positif, pembuatannya tentu melalui mekanisme pembuatan perundang-undangan, dan sekaligus melekat sifat *Ius Constitutum*, yakni menjadi hukum positif yang memberikan sanksi bagi peristiwa atau perbuatan kriminal yang menggunakan komputer. Dilihat dari peningkatan tindak kejahatan siber (*cyber crime*). Wakil Kepala Kepolisian RI Komisaris Jenderal Syafruddin mengatakan bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan

di dunia maya atau cyber crime. Syafruddin mengatakan bahwa data yang dihimpun pihaknya mendapati 90 juta kali serangan siber terjadi di Indonesia selama Januari hingga akhir Juni 2016.

Cyber crime di Indonesia tertinggi ke dua di dunia setelah Jepang. Total serangan cyber ini ada 90 juta," ujar Syafruddin saat memberikan pidatonya di acara yang diselenggarakan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) (Ramadhan, 2018).Tak hanya itu, ia juga membeberkan data dari Kementerian Komunikasi dan Informatika (Kemkominfo) yang merinci terdapat 800 ribu situs penyebar *hoaks* di internet yang telah diblokir sepanjang tahun 2015 hingga saat ini. "Ada juga data dari *cyber crime* Bareskrim Polri sejak tahun 2015 mencatat ada 100 ribu akun di Medsos yang menyebarkan *hate speech*, ungkapnya. Ia mengatakan bahwa perkembangan teknologi informasi saat ini justru menjadi 'pedang bermata dua' bagi pihak aparat keamanan. Di satu sisi dapat berdampak positif bagi kemudahan manusia, namun di sisi lain dapat menimbulkan berbagai ancaman bagi pertahanan negara.

Terlebih lagi, ancaman terorisme global saat ini tengah mengancam kedaulatan Indonesia karena bergerak melalui medium dunia maya dalam melakukan strategi penyerangan untuk menebar ancaman teror di masyarakat.

Peningkatan transaksi bisnis dan belanja secara online via internet yang sangat tinggi serta energi dan semangat pertumbuhan digital ini, sayangnya tidak diiringi dengan kesadaran pelaku bisnis dan masyarakat akan risiko dari serangan *cyber*. Bahkan sebuah laporan menunjukkan masyarakat Indonesia menempati peringkat pertama sebagai negara paling berisiko mengalami serangan *cyber*.



Gambar 1. Grafik Negara Paling Beresiko mengalami Serangan IT Security

Cyber Crime Indonesia adalah salah satu risiko yang terkait dengan penyelenggaraan kegiatan *internet banking* adalah kemungkinan terjadinya tindakan kriminal dengan memanfaatkan teknologi internet atau yang lebih dikenal dengan istilah *cyber crime* atau internet *fraud* atau penipuan melalui internet (Saputra, 2016; Danuri & Suharnawi, 2017).

Peningkatan tindakan kriminal dengan memanfaatkan teknologi internet (*malware, identity theft, internet abuse, hacking*) semakin sering hal ini terlihat dari berbagai kasus serangan *cyber* seperti pembobolan dan sinkronisasi token memperlihatkan tren pergeseran pola serangan *cyber,* yang tadinya menargetkan bisnis dan pemerintah, kini semakin gencar menargetkan konsumen secara langsung.

Dari dalam negeri, CNN Indonesia memberitakan bahwa kasus kejahatan di dunia maya atau *cyber crime* menjadi kasus paling banyak yang ditangani Ditreskrimsus Polda Metro Jaya di sepanjang 2016. Dari 1.627 kasus yang ditangani polisi, 1.207 kasus merupakan kasus *cyber crime*. Dari 1.207 laporan kasus tersebut, sebanyak 699 kasus telah diselesaikan (Buce, 2018).

Source : BSSN (Salsabila, 2020)

Gambar 2. Jumlah Serangan Siber Diindonesia Jan-Agus 2019-2020

Perubahan pola hidup masyarakat Indonesia di masa pandemi Covid-19 yang cenderung lebih banyak mengandalkan internet ternyata turut berimbas pada kenaikan jumlah upaya serangan siber. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta. Angka terbanyak dicatat pada Agustus 2020, di mana BSSN mencatat jumlah serangan siber di kisaran 63 juta, jauh lebih tinggi dibandingkan Agustus 2019 yang hanya di kisaran 5 juta. Baca

juga: Serangan Siber Meningkat Jelang Pilpres AS Kasubdit Identifikasi Kerentanan dan Penilaian Risiko Infrastruktur Informasi Kritikal Nasional III BSSN, Sigit Kurniawan, mengatakan kenaikan tajam jumlah serangan siber di Indonesia dipengaruhi langsung oleh perubahan pola hidup masyarakat selama pandemi. Karena pemakaian internet dan transaksi online semakin banyak, kata Sigit, pelaku kejahatan siber pun makin gencar melancarkan aksinya. "Saat pandemi, orang-orang makin sering transaksi digital. Kenaikan transaksi digital memicu para penjahat makin banyak," ujar Sigit. Data dari Kementerian Komunikasi dan Informatika (Kominfo) turut menunjukkan bahwa angka penggunaan internet di Indonesia selama pandemi memang meningkat hingga kisaran 40 persen. Peningkatan itu tak lain disebabkan oleh kebijakan *social distancing* yang membuat warga bekerja, belajar, dan melakukan berbagai aktivitas lain dari rumah lewat sambungan internet. Pusat penggunaan internet juga bergeser, dari tadinya berada di lingkungan perkantoran, kini menjadi lebih banyak di wilayah pemukiman. Pemakaian internet di daerah tertinggal turut naik sebesar 23 persen. Meskipun jumlah laporan serangan siber di Indonesia terkesan tinggi, Sigit menegaskan bahwa angka yang dicatat BSSN merupakan "upaya kejahatan", bukan serangan siber yang berhasil terjadi. Sigit menjelaskan, salah satu parameter yang dinilai BSSN sebagai serangan siber adalah kegiatan peretas yang melakukan *scanning* pada port situs yang terbuka dengan mengirimkan paket SYN *scan*. "Ada kegiatan yang tidak normal dan ini yang ditangkap oleh BSSN sebagai suatu serangan," pungkas Sigit (Salsabila, 2020).

2. Dasar Hukum Cyber Crime di Indonesia

Dasar hukum terkait dengan penanggulangan kejahatan siber di Indonesia merujuk pada beberapa peraturan yang telah ada. Pertama, adalah Undang-Undang Dasar 1945 yang mencantumkan Pasal 28G ayat (1) yang melindungi hak atas informasi dan komunikasi, sejalan dengan Pasal 28J ayat (1) yang menjamin hak untuk melindungi diri secara pribadi. Selanjutnya, terdapat berbagai pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang relevan dengan penanganan kejahatan siber, seperti Pasal 362 tentang pencurian yang dapat diterapkan dalam kasus carding . Carding merupakan kegiatan transaksi e-commerce dengan menggunakan nomor kartu kredit palsu atau curian, yang melanggar hukum pidana terkait pencurian (Teguh, 2008). Selain itu, Pasal 378 tentang penipuan dapat diterapkan dalam penipuan melalui website yang menawarkan barang palsu, sementara Pasal 311 tentang pencemaran nama baik relevan dalam kasus penyebaran informasi negatif melalui media internet. Pasal-pasal lain yang dapat diterapkan termasuk Pasal 303 tentang perjudian online dan Pasal 282 tentang pornografi online. Selain itu, terdapat undang-undang lain seperti Undang-Undang Hak Cipta, Undang-Undang Telekomunikasi, Undang-Undang Pemberantasan Tindak Pidana Terorisme, dan Undang-Undang Pencucian Uang yang juga dapat digunakan untuk menanggulangi kejahatan siber.

Dengan adanya dasar hukum yang kuat, diharapkan penegakan hukum terhadap kejahatan siber dapat dilakukan secara efektif untuk melindungi masyarakat dan keamanan siber negara.

3. Pencegahan dan Penanggulangan Cyber crime (kejahatan siber) Dari Kebijakan

Untuk menanggulangi maraknya kasus tindak pidana cyber crime (kejahatan siber), berbagai upaya penanggulangan telah dilakukan. Salah satu upaya tersebut adalah melalui sarana penal, yang melibatkan penerapan kebijakan dalam hukum pidana. Ini mencakup penerapan pidana materiil, hukum formil, dan penitentier dalam masyarakat untuk menegakkan aturan hukum. Selain itu, upaya juga dilakukan melalui sarana non-penal dengan memperbaiki perekonomian nasional, memberikan pendidikan budi pekerti kepada setiap individu, terutama kepada mereka yang rentan melakukan kejahatan, dan memperbaiki sistem kesehatan mental masyarakat. Kerjasama internasional dalam pemberantasan tindak pidana cyber crime juga ditingkatkan, bersama dengan perbaikan sistem pengamanan komputer. Selain itu, penguatan hukum administrasi dan hukum perdata yang terkait dengan pengelolaan sistem dan jaringan komputer juga menjadi bagian dari upaya penanggulangan kejahatan siber ini. Dengan mengimplementasikan berbagai kebijakan ini, diharapkan dapat mengurangi dan mencegah tindak pidana cyber crime serta meningkatkan kesadaran dan perlindungan terhadap masyarakat dan infrastruktur siber negara.

Metode

Dalam penelitian ini digunakan metode yuridis empiris dengan bahan primer, UUD 1945, KUHP dan UU No. 19 Tahun 2016 tentang perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, untuk bahan sekunder diambil dari buku, jurnal, internet, doktrin, artikel dan asas-asas hukum, pendapat hukum juga diperoleh melalui beberapa narasumber. Teknik Pengumpulan data adalah studi Kepustakaan dan wawancara dengan narasumber. Analisis data yang digunakan dalam penelitian ini adalah analisis secara kualitatif.

Hasil Dan Pembahasan

1. Hasil

Setelah dilakukan penelitian, ditemukan bahwa dalam penerapan aturan pemidanaan berdasarkan hukum pidana positif di Indonesia, yaitu sebagai berikut.

a. Penerapan dalam Pasal-Pasal KUHP, dalam perkara yang menjadikan komputer sebagai sasaran kejahatan dan perkara yang menggunakan komputer sebagai sarana kejahatan.

Dalam penanganan kasus tindak pidana cyber crime yang menyerang sistem komputer atau menggunakan komputer sebagai sarana kejahatan, penerapan hukum terhadap pelaku dilakukan dengan mengacu pada berbagai kategori. Pertama kategori pencurian, Pada Kasus ini empat terdakwa kasus skimming Bank BRI diganjar hukuman berbeda di Pengadilan Negeri (PN)

Kabupaten Kediri, kemarin. Paling berat, vonis terhadap Supeno, 44, warga Dusun Tambak, Desa Ngadi, Mojo yang didakwa otak pelakunya. terbukti secara sah dan meyakinkan melanggar UU Nomor 19/2016 sebagaimana perubahan dalam UU Nomor 11/2008 tentang Informasi dan Transaksi Elektronik (ITE). Supeno juga dijerat pasal 363 KUHP tentang pencurian dengan pemberatan. Penerapan UU yang sama juga diterima terdakwa Nur Mufid, 41. Namun, vonis pria asal Desa Sanirejo, Kecamatan Kaliwangu, Kendal, Jawa Tengah ini lebih ringan. Dari tuntutan JPU lima tahun penjara, majelis hakim mengganjarnya hukuman kurungan empat tahun. Sementara vonis dua terdakwa lainnya, Mustofa, 38, asal Dusun Tebokan, Desa Boro, Kedungwaru, Tulungagung, dan Sujianto, 50, warga Dusun Kedungringin, Desa Nguter, Pasirian, Lumajang lebih ringan. Jika sebelumnya, JPU menuntut tiga tahun enam bulan, kemarin, hakim mengganjarnya dengan hukuman dua tahun enam bulan atau 2,5 tahun. Keringanan hukuman itu lantaran peran keduanya tak terlalu vital. Dalam ksus tersebut, Mustofa dan Sujianto berperan sebagai pemasang alat skimming di anjungan Auto Teller Machine (ATM). Sedangkan Nur Mufid bertugas mengambil uang nasabah di ATM BRI tersebut. Mustofa dan Sujianto didakwa dengan pasal 46 ayat 2 UU Nomor 19/2016 perubahan UU Nomor 11/2008 tentang ITE dengan hukuman maksimal tujuh tahun penjara. Kasus skimming ini merugikan sekitar 400 nasabah BRI. Nilai kerugian mencapai Rp 2,2 miliar. Sedangkan ATM yang menjadi sasaran adalah ATM Diva Swalayan Ngadiluwih, ATM BRI di Jl.Doho, dan ATM BRI di RS Muhammadiyah Kediri.

Kedua kategori persaingan curang, dalam kasus ”Domain Name” PT Mustika Ratu Mahkamah Agung melalui Putusan Mahkamah Agung No. 1082 K./Pid./2002, tanggal 24 Januari 2003, memutuskan bahwa domain name mustika-ratu.com memenuhi delik pemalsuan curang sebagaimana diatur dalam Pasal 382 bis KUHP. Untuk itu, terdakwa (Chandra Sugiono) dijatuhi penjara selama 4 (empat) bulan. Putusan Mahkamah Agung ini membatalkan Putusan Pengadilan Negeri Jakarta Pusat yang dalam putusannya membebaskan terdakwa dari segala tuntutan. Pasal 382 :Barang siapa untuk mendapatkan, melangsungkan atau memperluas hasil perdagangan atau perusahaan milik sendiri atau orang lain, melakukan perbuatan curang untuk menyesatkan khalayak umum atau seseorang tertentu, diancam, jika perbuatan itu dapat menimbulkan kerugian bagi konkuren- konkurennya atau konkuren-konkuren orang lain, karena persaingan curang, dipidana penjara paling lama satu tahun empat bulan, atau pidana denda paling banyak tiga belas ribu lima ratus rupiah.

Ketiga kategori pemalsuan, terdakwa Petrus Pangkur dijatuhi pidana penjara selama 15 (lima belas) bulan oleh Pengadilan Negeri Sleman (Yogyakarta) karena terbukti secara sah dan meyakinkan melakukan tindak pidana pemalsuan melalui internet. Pelaku membeli barang dengan menggunakan kredit milik warga negara Amerika Serikat melalui perdagangan online (e-commerce). Ketentuan yang digunakan sebagai dasar mengadili terdakwa adalah Pasal 378

KUHP. Total harga barang yang dibeli adalah Rp.4.000.000,00 (empat juta rupiah). Waktu yang diperlukan untuk penyidikan kasus tersebut 8 (delapan) bulan (Widyopramono, 1994). Pasal 378 :Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

b. Penerapan Ketentuan Undang-Undang di Luar KUHP untuk Mengadili Perkara yang menjadikan Komputer sebagai Sarana Kejahatan.

Penerapan ketentuan undang-undang di luar Kitab Undang-Undang Hukum Pidana (KUHP) untuk mengadili perkara yang menggunakan komputer sebagai sarana kejahatan dilakukan dengan mengacu pada undang-undang yang khusus mengatur tentang informasi dan transaksi elektronik. Pertama Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta. Sebagai contoh konkret, dalam penanganan kasus antara PT. Inter Sport Marketing dan PT. Rahayu Pramid Biyany, Undang-Undang ini dijadikan acuan hukum. Dalam kasus tersebut, PT. Inter Sport Marketing sebagai penerima lisensi dari Federation International De Football Assotiation (FIFA) untuk media rights menyiarkan tayangan 2014 FIFA World Cup Brazil di seluruh wilayah Republik Indonesia. Namun, PT. Rahayu Pramid Biyany melakukan perbuatan melawan hukum dengan menayangkan acara tersebut di area komersial, yakni di Cakra Kusuma Hotel Yogyakarta, tanpa izin dari PT. Inter Sport Marketing. Sebagai akibatnya, pengadilan memutuskan untuk menghukum PT. Rahayu Pramid Biyany untuk membayar kerugian kepada PT. Inter Sport Marketing sejumlah Rp. 1.000.000.000,- (satu miliar rupiah), serta biaya perkara sejumlah Rp. 1.591.000 (satu juta lima ratus sembilan puluh satu ribu rupiah) sebagai bentuk pertanggungjawaban hukum atas pelanggaran hak cipta yang dilakukan. Dengan demikian, penerapan undang-undang tentang hak cipta menjadi instrumen penting dalam menegakkan hukum terkait penggunaan komputer sebagai sarana kejahatan dalam bidang ini.

Kedua Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Sebagai contoh yaitu pada penanganan kasus Dani Firmansyah. Dalam kasus Dani Firmansyah, terdakwa kasus pembobolan situs Tabulasi Nasional Komisi Pemilihan Umum (KPU), persidangan telah berlangsung pekan lalu di Pengadilan Negeri Jakarta Pusat. Jaksa Penuntut Umum (JPU) dalam perkara tersebut, yaitu Ramos Hutapea, menegaskan bahwa Dani didakwa melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan Telekomunikasi. Tindakan tersebut dianggap melanggar ketentuan Pasal 22 jo. 50 serta Pasal 38 jo. 55 Undang-undang No. 36 tahun 1999 tentang Telekomunikasi (UU Telekomunikasi). JPU menjelaskan bahwa perbuatan Dani termasuk penyerangan pada server milik Komisi Pemilihan Umum (KPU) yang terjadi pada

tanggal 17 April 2004. Dani melakukan akses ke jaringan tersebut melalui Internet Protocol (IP) Proxy Thailand yang berasal dari IP PT Danareksa. Ia kemudian menambahkan perintah-perintah yang mengakibatkan perubahan nama-nama partai politik dengan nama-nama buah-buahan dan nama-nama lainnya di situs KPU. Proses pengubahan nama-nama partai politik tersebut berlangsung antara pukul 11.24 lebih 16 detik hingga pukul 11.34 lebih 27 detik. Atas tindakannya, terdakwa yang membobol situs Komisi Pemilihan Umum, dituntut hukuman satu tahun penjara dan denda sebesar Rp.10.000.000 (Sepuluh Juta Rupiah), yang dapat diganti dengan tiga bulan kurungan jika denda tersebut tidak dibayarkan.

Ketiga Undang-undang Nomor 19 tahun 2016 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Sejak tanggal 21 April 2008,

Dalam Kasus Muhamad Tamim Pardede dengan nomor perkara 981 K/Pid.Sus/2018. Terdakwa terbukti bersalah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “Dengan sengaja dan tanpa hak, menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (SARA)” sebagaimana diatur dan diancam pidana dalam dakwaan Kesatu: Pasal 45A Ayat (2) jo Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016. Dan menghukum pidana penjara selama 3 (tiga) tahun dikurangi selama Terdakwa menjalani masa tahanan dan perintah agar Terdakwa tetap ditahan dan denda sebesar Rp. 200.000.000,00 (dua ratus juta rupiah) subsider 3 (tiga) bulan kurungan.

2. Pembahasan

Berdasarkan hasil penelitian di atas, ditemukan bahwa dalam penerapan aturan pemidanaan berdasarkan hukum pidana positif di Indonesia, terdapat beberapa aspek yang penting untuk diperhatikan. Pertama-tama, penerapan aturan ini terkait dengan penggunaan komputer sebagai sasaran kejahatan atau sebagai sarana kejahatan. Dalam beberapa kasus, terdapat penggunaan komputer yang melanggar hukum, seperti tindak pidana skimming pada Bank BRI. Pada kasus ini, terdapat beberapa terdakwa yang dijerat dengan Pasal 363 KUHP tentang pencurian dengan pemberatan. Vonis yang diberikan kepada terdakwa bervariasi tergantung pada peran masing-masing dalam kejahatan tersebut.

Kedua, terdapat kasus-kasus yang masuk dalam kategori persaingan curang, seperti kasus pemalsuan domain name. Dalam hal ini, hukum yang diterapkan mengacu pada Pasal 382 bis KUHP yang mengatur tentang pemalsuan curang. Pengadilan memberikan vonis penjara kepada terdakwa sebagai bentuk hukuman atas pelanggaran yang dilakukan.

Ketiga, terdapat kasus-kasus yang masuk dalam kategori pemalsuan, seperti kasus tindak pidana pemalsuan melalui internet. Dalam hal ini, hukum yang diterapkan mengacu pada Pasal

378 KUHP yang mengatur tentang penipuan. Pengadilan memberikan vonis penjara kepada terdakwa sebagai bentuk pertanggungjawaban hukum atas tindakan pemalsuan yang dilakukan.

Selanjutnya, penerapan ketentuan undang-undang di luar Kitab Undang-Undang Hukum Pidana (KUHP) untuk mengadili perkara yang menggunakan komputer sebagai sarana kejahatan dilakukan dengan merujuk pada undang-undang yang khusus mengatur tentang informasi dan transaksi elektronik. Contohnya adalah Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta, yang digunakan dalam kasus tindak pidana melanggar hak cipta. Dalam kasus ini, pengadilan menghukum terdakwa untuk membayar kerugian kepada pihak yang merasa dirugikan dan biaya perkara sebagai bentuk pertanggungjawaban hukum atas pelanggaran yang dilakukan.

Selanjutnya, terdapat penerapan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang digunakan dalam kasus tindak pidana pembobolan situs web. Dalam kasus ini, terdakwa dijerat dengan Pasal 22 jo. 50 serta Pasal 38 jo. 55 UU Telekomunikasi sebagai dasar hukum dalam pengadilan.

Kemudian, penerapan Undang-Undang Nomor 19 tahun 2016 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik juga penting dalam menangani tindak pidana di ranah digital. Contohnya adalah kasus menyebarkan informasi yang menimbulkan rasa kebencian atau permusuhan, yang diatur dalam undang-undang tersebut. Terdakwa dalam kasus ini dihukum pidana penjara dan denda sebagai bentuk pertanggungjawaban hukum atas tindakan yang dilakukan.

Dengan demikian, penerapan aturan pemidanaan dalam kasus-kasus cybercrime di Indonesia menggambarkan pentingnya penegakan hukum yang sesuai dengan perkembangan teknologi dan bidang informasi. Melalui penerapan hukum yang tepat dan adil, diharapkan dapat mencegah dan menindaklanjuti tindakan kriminal di ranah digital dengan lebih efektif.

Kesimpulan

Berdasarkan uraian yang telah disampaikan, dapat disimpulkan beberapa hal penting terkait dengan kejahatan siber di Indonesia. Pertama, terjadi peningkatan signifikan dalam jumlah serangan siber dari tahun ke tahun, yang menunjukkan eskalasi ancaman keamanan dalam ranah digital. Kedua, berbagai upaya penanggulangan telah dilakukan, baik melalui sarana penal maupun non-penal, namun masih diperlukan peningkatan kualitas dan efektivitas dalam menangani kejahatan ini. Sarana dan kebijakan yang ada diharapkan dapat memberikan respons yang lebih efisien dan efektif terhadap tindak pidana cyber crime, meskipun tidak dapat sepenuhnya mengatasi semua bentuk kejahatan siber. Oleh karena itu, perlu adanya upaya harmonisasi kebijakan pemidanaan dengan perkembangan teknologi informasi yang terus berubah, serta peningkatan teknologi informasi sebagai alat pemeriksaan yang lebih canggih

untuk menangani kejahatan siber yang bersifat transnasional. Dengan demikian, diharapkan dapat menciptakan lingkungan digital yang lebih aman dan terlindungi bagi masyarakat secara keseluruhan.

Referensi

Buce, D. (2018). *Waspadailah! Hantaman Serangan Cyber terhadap Indonesia*. Proxsisgroup; Penerbit Genesia. https://proxsisgroup.com/cyber-crime-indonesia/

Danuri, M., & Suharnawi, S. (2017). Trend cyber crime dan teknologi informasi di indonesia. *Jurnal Ilmiah Infokam*, *13*(2).

Pasal 26 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2016).

Ramadhan, R. (2018). *Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia*. CNN, Indonesia. https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia

R.Nitisbaskara, R. (2005). *Tegakkan Hukum gunakan Hukum*. Kompas.

Salsabila, P. Z. (2020). *Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi*. Kompas.Com. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. *2016 International Conference on ICT For Smart Society (ICISS)*, 1–5.

Savitri, A. (2009). *Revolusi Industri 4.0, mengubah tantangan menjadi peluang di Era Disrupsi 4.0*. Penerbit Genesia.

Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*. Raja Grafindo Persada.

Teguh, A. (2008). *Menjerat Pelaku Cyber Crime dengan KUHP, 'Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 3 Maret 2009'*.

Widyopramono. (1994). *Kejahatan di Bidang Komputer, Pustaka Sinar Harapan* (p. 67). Pustaka Sinar Harapan.