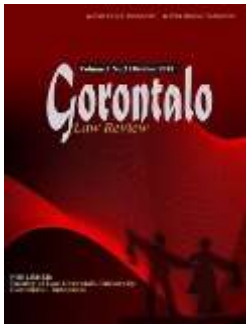
Gorontalo
Law Review
Volume 6 - NO. 2 – Oktober 2023
E-ISSN: 2614-5030 P-ISSN: 2614-5022



PENGATURAN TINDAK PIDANA CYBER CRIME DALAM HUKUM POSITIF DI INDONESIA

Jacky Robbinson Dyda
Fakultas Hukum Universitas Trisakti
samuelhudida@gmail.com

Elfrida Ratnawati
Fakultas Hukum Universitas Trisakti
elfrida.r@trisakti.ac.id

Abstrak

Teknologi terus berkembang dari masa ke masa tentunya mempunyai manfaat, disamping manfaat yang diberikan oleh teknologi terdapat pula dampak yang bersifat negatif. Dampak negatif tindak pidana teknologi dapat dirasakan siapa saja yang menggunakannya tanpa memandang bulu, dari masyarakat umum hingga kepada aparatur pemerintah. Tindak pidana teknologi memiliki berbagai macam modus oleh sebab itu penelitian ini memiliki tujuan agar dapat memberikan informasi terhadap klasifikasi-klasifikasi terhadap tindak pidana yang digunakan oleh teknologi informasi atau kejahatan cyber crime pada hukum pidana dan pengaturan dalam usaha terhadap pencegahan tindak pidana kejahatan teknologi informasi. Pada penelitian ini menggunakan metode yuridis normatif yakni bersifat studi kepustaan dengan mengumpulkan data-data, fakta, dan bahan bacaan primer Dengan tujuan mengetahui bagaimana hukum pidana dapat menyesuaikan diri dengan teknologi yang berkembang di Indonesia dan mengetahui jenis kejahatan apa saja yang ada pada bidang informasi berkaitan dengan teknologi yang mengadopsi ketentuan hukum pidana di Indonesia.

Kata Kunci : Hukum; Pidana; Teknologi; Informasi

Abstract

Technology continues to develop from time to time, of course, has benefits, besides the benefits provided by technology, there are also negative impacts. The negative impact of technology crime can be felt by anyone who uses it regardless of feathers, from the general public to government officials. Technology crimes have various modes, therefore this study aims to provide information on the classifications of criminal acts used by information technology or Cyber Crime in criminal law and regulations in efforts to deal with information technology crime crimes. In this study, a normative juridical method was used, which is a literature study by collecting data, facts, and primary reading materials with the aim of knowing how criminal law can adapt to the technology that is developing in Indonesia and knowing what types of crimes exist in the field of related information. with technology that adopts the provisions of criminal law in Indonesia.

Keywords: Law, Criminal, Technology, Information

1. PENDAHULUAN

Saat ini secara masif bidang dalam kehidupan yang dipengaruhi oleh kehadiran teknologi. Seiring dengan berjalannya waktu, teknologi dan informasi juga mengalami kemajuan. Teknologi dan informasi dapat dikatakan memiliki tujuan untuk memberikan kemudahan serta mempercepat pekerjaan. Piranti-piranti serta alat-alat yang dihasilkan dari perkembangan pengetahuan serta teknologi menawarkan kemudahan kepada umat manusia. Saat ini jarak dan waktu pada saat ini bukan lagi menjadi penghalang dalam melakukan sesuatu karena kehadiran teknologi dan informasi yang memberi kemudahan. Kebiasaan hidup masyarakan serta adanya perkembangan manusia secara menyeluruh juga ikut mengalami perubahan seiring dengan kehadiran teknologi informasi di tengah-tengah umat manusia. Perubahan sosial yang berubah dengan cepat yang seolah-olah dunia menjadi tanpa batas (*borderless*).(Akub, 2020)

Adanya kemajuan teknologi ini merupakan bagian dari budaya manusia itu sendiri yang memiliki dampak postif tapi juga tentu saja memiliki dampak negatif . menurut J.E Sahetapy, kejahatan memiliki kaitan yang erat serta telah ikut andil menjadi bagian dari budaya. Tingkat budaya yang tentunya semakin tinggi serta bangsa yang semakin modern berbanding lurus dengan semakin modern kejahatan dalam macam, sifat serta pelaksanaannya. Oleh karena itu selain daripada kemudahan yang dirasakan dalam kehadiran teknologi dan informasi, terdapat sisi negatif yang ikut bersamaan muncul ini menimbulkan kerugian dan korban dapat terjadi apabila teknologi disalahgunakan oleh seseorang. Penyalahgunaan teknologi ini biasanya memiliki tujuan serta maksud tertentu yang tentunya untuk mencapai tujuan yang menguntungkan dirinya sendiri maupun kelompok. (Darmadi et al., 2019)

Hal ini tentunya bersifat melawan hukum, apabila teknologi disalahgunakan oleh pelaku tindak pidana untuk mendapatkan korbannya. Salah satu modus dalam penyalahgunaan teknologi dan informasi yaitu modus penipuan undian berhadiah. Hal ini sudah umum diketahui oleh sebagian besar masyarakat yang menggunakan teknologi informasi, modus penipuan undian berhadiah melalui SMS (*Short Massage Service*) atau pesan singkat dengan media whatsapp. Modus operandi yang dilakukan oleh pelaku adalah jika korban ingin mendapatkan hadiah yang telah dijanjikan oleh pelaku tindak pidana, maka korban akan diarahkan pelaku untuk membayarkan sejumlah uang dengan beralasan uang yang harus dibayarkan

tersebut untuk kepentingan membayar pajak ataupun administrasi dari hadiah yang telah dijanjikan kepada korban. Selanjutnya jika korban telah memenuhi arahan dari pelaku, maka pelaku akan menghilang dan korban tidak akan mendapatkan apa yang telah dijanjikam oleh pelaku sebelumnya. (Nahak, 2017)

Cyber Crime dikategorikan sebagai tindakan serta perbuatan hukum secara nyata walau sifatnya virtual. Terlalu banyak yang akan lolos dari jerat hukum jika dilihat secara yuridis hukum konvensional sudah tidak ada tempat lagi dalam memasukkan kategori berdasarkan ukuran untuk dapat dijadikannya suatu objek serta dianggap sebagai perbuatan. Perbedaan terhadap *cyber crime* ini antara kejahatan konvensional yaitu terdapat peran teknologi yang dalam hal ini memberikan kemudahan untuk melakukan tindak kejahatan. Kegiatan virtual dalam dunia *cyber* tentu telah nyata dirasakan dampaknya, meskipun dalam hal alat bukti ini termasuk bersifat elektronik. Maka dari itu dalam memasukkan subjek pelaku tentu harus dikualifikasikan sebagai perbuatan hukum secara nyata yang dilakukan oleh seseorang.(Singgi et al., 2020)

Terdapat 2 (dua) faktor yang membuat *cyber crime* ini muncul sebagai tindak pidana yangmana disebabkan oleh teknis serta sosio ekonomi dalam masyarakat. Dalam segi teknis terdapat ketidakmerataannya penyebaran teknologi ini membuat ada pihak yang lebih canggih daripada pihak lain yang kurang memadai sehingga kelemahan tersebut dijadikan menjadi sarana untuk melakukan perbuatan tidak bertanggungjawab sehingga terjadinya kejahatan. Hal ini juga dipermudah lagi dengan jaringan yang saling terhubung antara jaringan lainnya sehingga pelaku bisa melancarkan aksinya. Lalu yang kedua terhadap faktor sosio ekonomi ini sendiri karena *cyber crimei* diartikan sebagai produk ekonomi. Banyak negara pada bidang komoditi ekonominya tentunya membutuhkan manfaat dari adanya penyebaran teknologi informasi ini, untuk itu keamanan jaringan (*security network*) menjadi isu yang sangat hangat. Komoditi ekonomi tentunya sangatlah membutuhkan keamanan jaringan. Dalam kegiatan besar perekonomian dunia ini tentunya *cyber crime* terus mengintai untuk ikut bagian.(Bellini & Sutabri, 2023)

Pada dasarnya tidak ada kekosongan hukum jika membahas persoalan mengenai *cyber crime*, namun ketika menyinggung tentang persoalan yang terjadi terdapat perbedaan pendapat. Contohnya ketika dalam penafsiran oleh Hakim dari suatu unsur pidana yang memenuhi dalam suatu aturan ditafsirkan sebagai masuk kedalam kategori penipuan tapi ternyata ada pula yang memasukan kedalam klasifikasi sebagai pencurian. Berkaca atas persoalan ini perlu sekali dikembangkannya pemahaman para Hakim dalam menafsirkan dalam dunia teknologi informasi, agar tidak menjadi persoalan ambigu yang membingungkan. Karena kembali lagi kepada *cyber crime* yang merupakan dimensi baru dalam bidang hukum.(Ali, 2014)

Terdapat penelitian sebelumnya yang membahas seputar artikel ini, Penelitian Pertama di kemukakan oleh Musa Darwin Pane yang berjudul " Penegakan Hukum Cyber Crime dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi " melalui Jurnal Loyalias Sosisal Tahun (Pane & Situmeang, 2021)dalam penelitian ini hanya membahas mengenai kerugian yang di alami korban dan memaparkan seputar kebijakan yang dilakukan oleh aparat penegak untuk dapat mencegah tindak pidana cyber crime. Penelitian kedua yakni Muhammad Anthony Aldriano (Aldriano & Priyambodo, 2022) dengan penelitian berjudul "Cyber Crime dalam Sudut Pandang Pidana" melalui Jurnal Kewarganegaraan Tahun, adapun perbedaan pada penelitian ini yakni penelitian ini membahas seputar penanggulangan cyber crime oleh ketentuan pidana yang dimuat di dalam KUHP. Yang ketiga penelitian yang di garap oleh Indriani Berlian Mewengkang

(Mewengkang et al., 2021)mengenai "Kajian Yuridis Cyber Crime Penanggulangan dan Penegakan Hukumnya" pada kali ini dibahas mengenai penegakan pelaku yang melakukan perbuatan cyber crime, adanya hukum hadir sebagai upaya penanggulangan kejahatan di bidang teknologi informasi saja.

Kebaharuan penelitian ini dengan penelitian yang dibahas sebelumnya yaitui membahas terkait keefektifan dalam penegakan hukum pidana terdahap *cyber crime* ini dipandang dari semua unsur, serta penelitian ini merujuk kepada KUHP dan membahas berkenaan dengan sanksi yang diancamkan terbilang ringan untuk kejahatan *cyber* yang bisa menimbulkan kerugian yang besar. Tentu ini sangat tidak sepadan apabila kerugian itu terjadi. Sehingga dengan demikian hukum positif harus dapat menjamin perlindungan terhadap korban cyber crime ini.

2. METODE PENELITIAN

Metode pendekatan yang diadopsi oleh penulis untuk melakukan kegiatan penelitian ini ialah berpegang kepada metode normatif yuridis. Maka adanya penelitian hukum yang bersifat normatif ini merujuk kepada arah fokus artikel untuk memberikan fokusnya kepada reverensi berupa data kepustakaan yang merupakan bagian dari proses penelitian meliputi bahan sekunder. Bahan sekunder ini berisi data primer maupun bahan hukum sekunder dan juga bahan hukum tersier. Data sekunder ini meliputi peraturan, terhubung pada regulasi yang ada di Indonesia serta mengacui pada Kitab Undang-Undang Hukum Pidana dan studi kepustakaan lainnya. Penelitian ini mencakup kepada sudut pandang pidana melihat kejahatan teknologi dan informasi berdasarkan ketentuan hukum positif sesuai dengan peraturan di Indonesia. (Efendi & Ibrahim, 2018)

3. PEMBAHASAN

a. Cyber Crime dalam Hukum Positif di Indonesia

Salah satu bentuk kejahatan dalam dunia globalisasi saat ini yang menjadi sorotan di dunia internasional ialah *cyber crime* atau yang dikenal dengan kejahatan teknologi dan informasi. Vodymyr Golubev memberikan julukan *New form of behavior anti sosial*. Serta adapun terdapat banyak istilah lainnya agar dapat dilekatkan kepada hal ini yakni kejahatan dunia maya *cyber space* dan *virtual space offence* yang merupakan dimensi baru bersumber dari *high tech crime*, bentuk baru terhadap *transnasional crime*, serta bentuk baru dalam lingkup *white collar crime*.

Kejahatan di dalam lingkup dunia maya atau yang kita ketahui sama-sama sebagai *cyber crime* ini sebuah bidang kejahatan yang dalam melakukan kegiatannya melalui media komputer dan jaringan. Alat utama dalam melakukan kejahatan *cyber crime* ini adalah komputer, namun adapun komputer yang dijadikan target dalam aksi kejahatan ini. Dapat dikatakan juga *cyber crime* merupakan kejahatan yang lahir akibat teknologi internet yang disalahgunakan. Inti dari pengertian tersebut yakni merupakan perbuatan melawan hukum atau terhubung pada kategori tindak pidana yang dengan kegiatannya beralaskan media internet yang didasari oleh kemampuan dari teknologi komputer serta jaringan telekomunikasi.(Febriansyah, 2022)

Beberapa ahli memiliki pandangan yang tidak sama di dalam mengartikan *cyber crime*. Dalam buku "Bunga Rampai Hukum Pidana", Muladi memberikan pendapatnya yaitu dari kacamata *cyber crime* ialah dapat dilakukan dengan pendakatan *computer crime*. Disamping itu ada pendapat bahwa apa yang dimaksud dengan *cyber crime* dan *computer crime* itu bukan lah suatu hal yang sama melainkan suatu hal yang berbeda. Pada kenyataannya terdapat usaha dalam memberikan arti yang luas terhadap pengertian komputer agar dapat mencakup

berbagai macam alat yang digunakan sebagai media untuk melakukan kejahatan dalam dunia *cyber.*(Widayanti, 2022)

Dalam hukum positif Indonesia, cyber crime diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini membahas tentang landasan hukum yang diatur penggunaan teknologi informasi dan transaksi elektronik di Indonesia. Adapun ketentuan yang diatur mengenai Akses ilegal (Pasal 30): Melarang akses yang tidak sah terhadap sistem komputer, baik dengan cara meretas, mengubah, atau menghapus data tanpa izin dari pemilik atau pengelola sistem. Pengintersepsi dan/atau perekaman data (Pasal 31): Melarang pengintersepsi atau perekaman data elektronik tanpa izin dari pemilik atau pengguna data tersebut. Penyebaran konten yang melanggar (Pasal 27 ayat (3)): Melarang penyebaran konten yang mengandung penghinaan, fitnah, pornografi anak, atau kekerasan melalui media elektronik. Penipuan online (Pasal 48): Melarang tindakan penipuan yang dilakukan melalui internet atau media elektronik lainnya.Serangan terhadap keamanan sistem elektronik (Pasal 32): Melarang melakukan tindakan yang mengganggu atau merusak sistem komputer atau jaringan komunikasi elektronik, seperti serangan DDoS (Distributed Denial of Service) atau serangan malware. Pencemaran nama baik (Pasal 27 ayat (1)): Melarang penyebaran informasi yang mencemarkan nama baik seseorang melalui media elektronik.

Dalam UU ITE, sanksi pidana yang diancamkan untuk pelanggaran-pelanggaran tersebut meliputi denda dan/atau pidana penjara. Besar denda dan lamanya pidana penjara tergantung pada jenis pelanggaran dan tingkat keparahannya. Selain UU ITE, terdapat juga undang-undang lain yang dapat diterapkan dalam kasus-kasus cyber crime, seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang memberikan penegasan mengenai tindakan pembajakan software dan hak kekayaan intelektual dalam dunia maya .Pemerintah Indonesia terus mengkaji dan mengkonsolidasikan hukum terkait cyber crime untuk menanggapi perkembangan teknologi dan tantangan baru yang muncul dalam dunia maya.

Namun berkenaan sanksi cyber crime pada KUHP ini dinilai tidak efektif. Meskipun ada perdebatan mengenai sanksi pidana yang diberlakukan dalam UU ITE ini, penting untuk diingat bahwa hukum dan peraturan berkembang seiring waktu. Pemerintah dan lembaga terkait dapat memperbarui dan memperkuat peraturan tersebut sama dengan jumlah kebutuhan maupun rintangan yang dialami di dalam dunia maya. Sanksi pidana yang diatur dalam UU ITE saat ini termasuk denda dan/atau pidana penjara. Denda yang diatur bervariasi tergantung pada jenis pelanggaran dan dapat mencapai jumlah yang signifikan. Sementara itu, hukuman penjara yang diatur dalam UU ITE berkisar antara beberapa bulan hingga beberapa tahun, tergantung pada tingkat pelanggaran. Namun, setiap peraturan dan hukuman memiliki pertimbangan dan tujuan tertentu. Sanksi pidana yang dijatuhkan dalam kasus cyber crime harus seimbang dan mempertimbangkan berbagai faktor, termasuk tingkat pelanggaran, potensi kerugian yang ditimbulkan, dan niat pelaku. Pemerintah Indonesia terus memantau perkembangan teknologi informasi dan komunikasi serta tantangan yang muncul di dunia maya. Jika terdapat kebutuhan untuk meningkatkan sanksi pidana dalam kasus cyber crime, pemerintah dapat mengambil langkah-langkah untuk memperkuat peraturan yang ada atau mengeluarkan peraturan baru yang sesuai dengan keadaan saat ini.(Ratulangi et al., 2021)

b. Kejahatan Cyber Melalui Sudut Pandang Pidana

Jika terdapat suatu tindakan kejahatan yang dirumuskan dalam suatu delik atau tindak pidana, maka dalam hukum pidana pelanggarnya akan dijatuhi pidana. *Strafbaarfeit* yang merupakan istilah tindak pidana yangmana dalam basa Belanda terdiri atas kata *Strafbaar* yang memiliki arti dapat dihukum serta *Feit* yang memiliki arti sebagian dari sebuah kenyataan. Para ahli hukum memberikan kesimpulannya sebagai berikut Hazewinkel Berpendapat bahwa *strafbaarfeit* ialah telah ditolaknya suatu perilaku manusia didalam pergaulan hidup pada masa tertentu serta hukum pidana harus memaksa perilaku tersebut ditiadakan karena sifat hukum pidana yang memaksa. Sedangkan menurut Pompe Suatu tindakan jika melihat kepada rumusan Undang-Undang didalamnya dan telah menyatakan hal tersebut merupakan suatu tindakan yang patut dihukum adalah pemahaman dari *strafbaarfeit.* Sedangkan menurut Simons *Strafbaarfeit* adalah keadaan ketika seseorang telah melakukan dengan sengaja suatu tindakan yang dimana didalam tindakan tersebut telah melanggar hukum maka atas dasar tindakan tersebut bisa untuk dimintai pertanggungjawaban kepada orang yang disangkakan berlandaskan pada undang-undang yang telah mencantumkan bahwa tindakan tersebut dapat dihukum karena telah memenuhi unsur perbuatan melawan hukum. (Diniyah, 2022)

Sedangkan menurut Simons *Strafbaarfeit* ialah ketika suatu tindakan yang patut dihukum apabila jika terdapat suatu hal yang di dalam undang-undang yangmana merupakan suatu larangan ataupun merupakan sebuah kewajiban yang telah dilalaikan. Jika semua unsur delik dalam apa yang dirumuskan oleh undang-undang telah terpenuhi semuanya maka tindakan tersebut dapat dihukum. inti dari apa yang di maksud dengan *Onrechtmatige handeling* ialah merupakan suatu tindakan melawan hukum pada saat *strafbaarfeit* menjadi pelanggaran kepada larangan atau kewajiban di dalam undang-undang.

Dapat disimpulkan ketika adanya kegiatan yang dengan melawan hukum dilakukan oleh seseorang maka atas dasar tindakan dari apa yang ia lakukan itu dapat dijatuhkan kepadanya suatu sanksi pidana berdasarkan hukum yang berlaku. Perkembangan lebih lanjut terhadap perbuatan melawan hukum atau yang disebut dengan tindak pidana dengan memanfaatkan teknologi komputer sebagai alat yang menjadi media untuk melakukan perbuatan yang merupakan kualifikasi dari *cyber crime* dapat menjadi dimensi baru dalam dunia pidana. Melihat kepada perspektif dalam hukum, kejahatan cyber ini tidak juga dikatakan kejahatan baru. Pelaku hanya melakukan pengembangan pada media kejahatannya. Konsep yang dilakukan dari tindak pidana ini hanya memiliki cara yang kurang lebih sedikit berbeda.

Dalam dunia kriminal sendiri, *cyber crime* dapat dikatakan sebagai kategori yang baru. Seperti halnya dalam KUHP sendiri telah mempunyai yurisdiksi yang secara jelas dapat dilihat dalam Pasal 2 KUHP yakni terdapat kententuan yang menyebut terhadap setiap orang di Indonesia yang telah melakukan suatu delik dapat diberikan kepadanya pidana yang dilekatkan ancaman sanksi pidana seusai dengan perundang-undangan yang berlaku di Indonesia. Menurut penulis adanya kata “setiap orang di Indonesia” merupakan hambatan untuk melakukan penegakan terhadap hukum *cyber crime* ini, karena dapat sekali dimungkinkan bahwa pelaku tidak berada di dalam wilayah negara Indonesia sedangkan yang menjadi korban berada di wilayah Indonesia. Perjanjian *mutual legal assistant* pada bidang hukum pidana atau biasa dikenal dengan ekstradisi ini seperti belum mampu dilakukan oleh negara kita akibat adanya Pasal 2 KUHP ini.(Djanggih, 2013)

Terdapat berbagai macam kategori dari *cyber crime* yakni sebagai berikut seperti *Joy Computing y*akni merupakan penggunaan komputer yangmana bukan

miliknya sendiri namun merupakan milik orang lain secara tanpa izin, masuk kedalam pencurian waktu pengoperasian komputer.*Hacking* Ialah kegiatan membuka dengan cara yang tidak sah atau bisa dikatakan tanpa adanya izin menggunakan alat yang melekat kepada terminal. Atau dapat dikatakan kegiatan menerobos dari program komputer yang dimiliki bukan olehnya sendiri yaitu milik orang lain. *The Trojan Horse* Perbuatan yang bertujuan untuk kepentingan pribadi ataupun orang lain dengan cara memanipulasi data ataupun perintah dalam suatu program, menghapus, atau bahkan menambah, serta menjadikannya tidak bisa dipergunakan. *Data Leakage m*elakukan pembocoran data yang semestinya harus dirahasiakan namun dibocorkan. Data tersebut bisa merupakan rahasia negara, perusahaan ataupun seseorang yang dipercayakan untuk memegang data dalam suatu kondisi atau situasi. *Data Diddling p*erbuatan yang didalamnya melakukan pengubahan data yang valid atau sah melalui cara yang tidak, ataupun bahkan melakukan penginputan data serta melakakukan output data. *To Frustate data communication* (*Verijdeling Data Communicatie*) melakukan penyia-penyiaan data terhadap komputer atau menggagalkan. *Software Piracy* Pembajakan hak cipta yang ada pada perangkat lunak, yang mana hak cipta ini telah dilindungi oleh HAKI. *Cyber Espionage* Memiliki definisi perbuatan secara diam-diam atau memata-matai pihak lain yang menjadi sasarannya melalui cara meretas jaringan dan sistem yang dimilikinya (*computer network system*) dengan memanfaatkan jaringan internet. *Spyware* atau program mata-mata yang kita kenal biasanya akan disipipkan ke dalam suatu perangkat. Data-data penting yang telah *computerized* biasanya merupakan sesuatu yang diincar dalam kejahatan ini. (Astuti, 2013)

Infringements of Privacy Informasi seseorang yang sangatlah rahasia biasanya adalah sasaran dari kejahatan siber ini. Kejahatan ini memiliki maksud untuk mengetahui bahkan mengambil keterangan pribadi seseorang dalam formulir yang telah terarsip secara dalam sistem *computerized*, yangmana tentunya hal ini sangat merugikan korban baik kerugian secara materil maupun kerugian immateril karena bisa saja nomor kartu kredit bahkan PIN dari ATM korban diketahui ataupun riwayat penyakit yang tersembunyi dan lain sebagainnya. *Data Forgery t*indakan kejahatan dimana dalam melakukan kegiatannya dilalui melalui pemalsuan dari data dokumen-dokumen penting korban dimana dokumen itu telah ada yang memiliki bentuk *scriptless* dokumen pada internet. Contoh dari tindak pidana dalam kategori ini biasanya terjadi pada dokumen-dokumen yang berkaitan dengan platform online dimaksudkan apabila terjadinya salah ketik yang dilakukan oleh korban maka akan memberikan keuntungan bagi pelaku.

c. Pengaturan Cyber dalam Hukum Pidana

PBB juga pernah memberikan himbauan melaui Kogres PBB VIII untuk para anggotanya melakukan penanggulangan kepada tindak pidana kejahatan *cyber crime* dengan melalui saran penal (*penal policy*). Hal ini tentu dalam penerapannya tidak mudah, dikarenakan pada zaman globalisasi seperti saat ini kejahatan tindak pidana siber (*cyber crime*) sangat menjadi keresahan yang dirasakan oleh masyarakat khususnya yang menggunakan teknologi dan infromasi dalam perangkat-perangkat sistem informasi jaringan. Menjadi suatu kebutuhan yang sangat dirasa penting demi melindungi pengguna serta memberikan perlindungan hukum terhadap mereka yang telah dirugikan.(Sartika et al., 2020)

Upaya terhadap pembuatan *cyberlaw* untuk Indonesia sendiri telah ada sejak tahun 1999. Payung hukum yang menjadi fokus utamanya saat itu ialah seputar perlindungan hukum yang generik dan menyinggung sedikit tentang transaksi elektronik. Lahirnya Undang-Undang nomor 36 Tahun 1999 tentang Telekomunikasi memiliki ancaman pidana penjara maksimal 6 (enam) tahun atau denda maksimal senilai Rp. 600.000.000 (enam ratus juta rupiah). Pada saat

disahkannya Undang-Undang Nomor 11 Tahun 2008 mengatur Informasi dan Transaksai Elektronik, berdampak ketidak berlakuannya lagi Undang-Undang Nomor 36 Tahun 1999 karena dianggap sudah tidak lagi dapat menghukum para pelaku tindak pidana.(Darmadi et al., 2019)

Dalam apa yang dituangkan di Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memiliki tujuan dapat mengharmonisasikan terhadap instrumen peraturan hukum nasional dengan hukum internsional tentunya berkaitan dengan teknologi informasi. Terhadap perubahan Undang-Undang Nomor 11 Tahun 2008 dengan Undang-Undang Nomor 19 Tahun 2016 memiliki capaian agar terjaminnya pengakuan atas penghormatan terhadap hak serte kebebasan orang lain dalam memberikan pemenuhan tuntuan kepastian hukum.(Malunsenge et al., 2022)

Definisi dari pengertian yang memiliki arti luas tentang kejahatan cyber yakni perbuatan pidana yang dalam perbuatannya melalui sarana ataupun dibantu dengan sesuatu yang berasal dari Sistem Elektronik berdasarkan melihat kepada Kitab Undang-Undang Hukum Pidana (KUHP). Maka artinya ketika perbuatannya melalui media atau bantuan dari Sistem Elektronik, perbuatan seperti dalam halnya pembunuhan, bahkan perdangan orang dapat ikut kedalam kualifikasi kejahatan *cyber* dalam makna yang luas menurut hukum pidana (KUHP). Adanya yang berpandangan bahwa hukum pidana dalam KUHP ini tidak dimungkinkan untuk menjangkau kejahatan ini, namun adapun sebagaian lainnya yang beranggapan bahwa hukum yang berlaku dapat untuk menyentuh kejahatan ini. Membahasa daripada perspektif hukum pidana terhadap tindak pidana kejahatan siber (*cyber crime*) ini maka penulis akan menghubungkannya dengan bentuk yang telah dimuat pada KUHP.(Putra, 2019)

Dalam kejadian *deface* atau bahkan *hacking* yang mengakibatkan kerusakan atau bukan segaimana fungsinya terhadap tatanan kepemilikan pihak lain, yakni pada program yang menjadi tidak dapat berfungsi atau tidak dapat digunakan sebagai mana fungsinya dapat digunakan maka memenuhi unsur pidana didalam Pasal 406 KUHP.

Beberapa contoh kasus berdasarkan jenis-jenis tindak pidana siber (*cyber* crime) yang diberikan oleh penulis, terlihat bahwa masih ada yang sebenarnya kekurangan dalam hal upaya penegakan hukumnya, sanksi yang diancaman KUHP apabila dijatuhkan masih dirasa terlalu ringan. Karena beberapa dari kasus yang berkaitan denga *cyber crime* menyebabkan kerugian yang sangat besar sehingga apabila ancaman hukuman itu dikenakan akan dirasa tidak sepadan terhadap kerugian yang telah ditimbulkan. Selain itu, penafsiran yang luas sangat dibutuhkan dalam delik dalam *cyber crime* yang termuat pada KUHP.

Menurut Seodjono Dirjosisworo jiika dilihat dari kacamata pidananya yakni : "Perubahan serta penyusuaian dalam lingkup sosial dan perkembangan terhadap teknologi yang sudah berjalan dalam kurun waktu setengah abad sejak tahun 1985 (Undang-Undang Nomor 73 Tahun 1958), yang terjadi dalam waktu yang cepat dengan mengalami perkembangan yang pesat serta zaman globalisasi telah menghadirkan teknologi informasi yang selalu mengalami perubahan. Untuk tentu dirasa Kitab Undang-Undang Hukum Pidana yang eksistensinya sudah cukup lama tidak mampu lagi untuk mengakomodir serta memberikan antipasi terhadap terjadinya tindak pidana yang mengalami peningkatan secara kualitatif dan kuantittatif berdasarkan dengan jenisnya, pola serta modus operandi yang tentunya tidak ada di dalam Kitab Undang-Undang Hukum Pidana". hal tersebut tentu sejalan dengan KUHP agar tidak banyak mengakomodir lagi tindak pidana *cyber crime.*(Prasetiyo & Zuhdy, 2020)

Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, mengkualifikasikan beberapa kegiatan yang termasuk dalam kejahatan di dunia maya, yaitu antara lain sebagai berikut Pada Pasal 16 yaitu, kejahatan terhadap nama domain; Pada Pasal 19 yaitu, kejahatan terhadap HAKI (hak kekayaan intelektual) dan hak atas informasi yang bersifat rahasia pada kehiatan teknologi informasi; Pada Pasal 22 yaitu, kejahatan terkait hak-hak pribadi; Pada Pasal 41 yaitu, kejahatan pornografiAdapun pada kenyataannya terdapat kejahatan dalam dunia siber yang belum masuk kedalam kategori suatu tindak pidana di peraturan perundang-undangan, namun perbuatan ini dapat dikriminalisasikan apabila telah merugikan masyarakat demi kepastian hukum.

4. PENUTUP

Perbuatan melawan hukum atau yang dikenal dengan tindak pidana ini memiliki perkembangan yang lebih lanjut dengan memanfaatkan teknologi komputer menjadi sarana-prasarana untuk melancarkan aksi tindak pidana ini merupakan dimensi baru dalam dunia tindak pidana yang dikenal sebagai *cyber crime.* Sudut pandang dari dalam hukum sendiri tidak juga dikatakan memandang *cyber crime* sebagai kejahatan yang baru melainkan pelaku memberikan pengembangan dalam sarana kejahatannya, namun konsep yang dilakukan dalam tindak pidana ini tetaplah sama mengalami sedikit perkembangan yangmana dapat dilihat dari aktifitas dan motif pelaku kejahatan ini. Secara yuridis sendiri belum dapat memiliki defiinisi yang rigit terhadap *cyber crime*. Ada yang berpendapat bahwa *cyber crime* berkaitan erat degan computer crime dan adapun sebagaian lainnya memiliki pendapat yang berbeda dalam mengartikan antara *cyber crime* dengan computer crime. Hal ini dipandang karena tidak semua *cyber crime* menggunakan computer sebagai medianya.

5. DAFTAR PUSTAKA

Akub, M. S. (2020). PENGATURAN TINDAK PIDANA MAYANTARA (CYBER CRIME) DALAM SISTEM HUKUM INDONESIA. *Al-Ishlah : Jurnal Ilmiah Hukum*, *21*(2). https://doi.org/10.33096/aijih.v20i2.19

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1).

Ali, D. (2014). Perlindungan Korban Tindak Pidana Cyber Crime Dalam Sistem Hukum Pidana Indonesia. *Pascasarjana Universitas Syiah Kuala*, *9*(1).

Astuti, D. P. (2013). Implementasi Penyidikan Tindak Pidana Cyber Crime Berkaitan Dengan Penjualan Barang Yang Tidak Sesuai Dengan Perjanjian Dalam Rangka Perlindungan Konsumen (Studi di Polda Jawa Timur). *Universitas Brawijaya Malang*.

Bellini, Y., & Sutabri, T. (2023). Sistem Pakar Mendeteksi Tindak Pidana Cyber Crime untuk Penanganan Komputer Forensik Menggunakan Backward Chaining. *Jurnal Digital Teknologi Informasi*, *6*(1). https://doi.org/10.32502/digital.v6i1.5619

Darmadi, Yusa, A., & Purwani, S. (2019). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online (Studi Kasus Unit Cyber Crime). *Jurnal Kertha Wicara*, *8*(10).

Diniyah, K. J. (2022). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing. *Dinamika: Jurnal Ilmiah Ilmu Hukum*, *28*(5).

Djanggih, H. (2013). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan. *Jurnal Media Hukum*, *I*(2).

Efendi, J., & Ibrahim, J. (2018). Metode Penelitian Hukum Normatif dan Empiris. In *Kencana* (Vol. 2, Issue Hukum).

Febriansyah, R. Y. (2022). DELIK-DELIK DILUAR KUHP (TINDAK PIDANA CYBER CRIME DAN CARA PENANGGULANGAN). *JHP17 (Jurnal Hasil Penelitian)*, *6*(2). https://doi.org/10.30996/jhp17.v6i2.6216

Malunsenge, L. M., Dj Massie, C., & Rorie, R. E. (2022). PENEGAKAN HUKUM TERHADAP PELAKU DAN KORBAN TINDAK PIDANA CYBER CRIME BERBENTUK PHISING DI INDONESIA. *LEX CRIMEN*, *11*(3).

Mewengkang, I. B., Warong, R. N., & Kuntag, M. (2021). Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya. *Lex Crimen*, *10*(5).

Nahak, S. (2017). Hukum Tindak Pidana Mayantara (Cyber Crime) dalam Perspektif Akademik. *Jurnal Prasada*, *4*(1).

Pane, M. D., & Situmeang, S. M. tua. (2021). Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi. *Jurnal Loyalitas Sosial: Journal of Community Service in Humanities and Social Sciences*, *3*(2). https://doi.org/10.32493/jls.v3i2.p93-105

Prasetiyo, P., & Zuhdy, M. (2020). PENEGAKAN HUKUM OLEH APARAT PENYIDIK CYBER CRIME DALAM KEJAHATAN DUNIA MAYA (CYBER CRIME) DI WILAYAH HUKUM POLDA DIY. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(2). https://doi.org/10.18196/ijclc.v1i2.9611

Putra, B. K. B. (2019). KEBIJAKAN APLIKASI TINDAK PIDANA SIBER (CYBER CRIME) DI INDONESIA. *Pamulang Law Review*, *1*(1). https://doi.org/10.32493/palrev.v1i1.2842

Ratulangi, C. H., Wahongan, Dr. A. S., & Mewengkang, F. R. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *IX*(5).

Sartika, R., Siregar, S. A. I., & Kartika Sari, N. P. R. (2020). KEKHUSUSAN PROSES PENYIDIKAN TINDAK PIDANA CYBER CRIME. *Jurnal Aktual Justice*, *5*(1). https://doi.org/10.47329/aktualjustice.v5i1.519

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2). https://doi.org/10.22225/jkh.2.1.2553.334-339

Widayanti, P. W. (2022). TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI CYBER CRIME. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *2*(2).