

# ANALISIS KEBIJAKAN CYBER CRIME DALAM HUKUM POSITIF DI INDONESIA

**Intan Permata Sari \*<sup>1</sup>**

Universitas Bandar Lampung, Indonesia

[intanpermatasarinaruto12345@gmail.com](mailto:intanpermatasarinaruto12345@gmail.com)

**Irma Wati Pasaribu**

Universitas Bandar Lampung, Indonesia

[irmawatipasaribu347@gmail.com](mailto:irmawatipasaribu347@gmail.com)

**Muhammad Zahien Akbar AS**

Universitas Bandar Lampung, Indonesia

[zahienakbar20@gmail.com](mailto:zahienakbar20@gmail.com)

**Berlian Cikka Octanelsha**

Universitas Bandar Lampung, Indonesia

[b.cikkaoctanelsha@gmail.com](mailto:b.cikkaoctanelsha@gmail.com)

## **Abstract**

*Technological developments move in line with the legal dynamics that occur in Indonesia. Information and communication technology has a huge impact on the regulatory revolution as well as social, cultural and community life. Apart from the positive impacts that can result from technological developments, there are also negative impacts, namely social media crimes or known as cyber crimes. Legitimate control over cyber crime is a challenge for cybercrime which is developing with the information technology revolution. Policy regarding cyber crime in positive law in Indonesia is the aim of writing this research. The research method used in this research is a normative legal approach. Data processing is carried out through library research, such as literature and scientific works related to research problems. The results of this research show that there are more than 7 regulations in the form of special laws and regulations in the Criminal Code (KUHP) which regulate cyber crime, then other policies are in Law no. 11 of 2008 as amended in Law Number 19 of 2016 concerning Information and Electronic Transactions.*

**Keywords:** Analysis, Policy, Cyber Crime, Indonesian Positive Law.

## **Abstrak**

Perkembangan teknologi bergerak seiring dengan dinamika hukum yang terjadi di Indonesia. Teknologi informasi dan komunikasi memiliki dampak yang sangat besar bagi revolusi regulasi dan juga kehidupan sosial, budaya, serta masyarakat. Selain dampak positif yang dapat dihasilkan dari adanya perkembangan teknologi juga terdapat dampak negatif yaitu merupakan kejahatan sosial media atau dikenal dengan kejahatan mayantara (*cyber crime*). Kendali yang sah atas *cyber crime* adalah sebuah tantangan bagi kejahatan mayantara ini yang ikut berkembang dengan revolusi teknologi informasi. Kebijakan mengenai kejahatan mayantara (*cyber crime*) dalam hukum positif di Indonesia merupakan tujuan dalam penulisan penelitian ini. Metode penelitian yang digunakan dalam penelitian ini adalah pendekatan hukum normatif.

---

<sup>1</sup> Korespondensi Penulis

Pengolahan data yang dilakukan melalui studi kepustakaan (*Library research*) seperti literatur dan karya ilmiah yang berkaitan dengan permasalahan penelitian. Hasil dari penelitian ini menunjukkan bahwa terdapat lebih dari 7 regulasi berupa peraturan perundang-undangan khusus di dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur mengenai kejahatan dunia maya atau cyber crime, kemudian dalam kebijakan lain terdapat pada Undang-Undang No. 11 Tahun 2008 sebagaimana diubah dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

**Kata Kunci:** Analisis, Kebijakan, Cyber Crime, Hukum Positif Indonesia.

## Pendahuluan

Teknologi informasi telah berkembang pesat di Indonesia dan negara-negara lain. Teknologi informasi telah mendorong pertumbuhan ekonomi dan akuisisi informasi global. Kejahatan dunia maya telah meningkat seiring dengan kemajuan teknologi informasi. Teknologi telah mengubah peradaban menjadi komunitas global. Perubahan ini disebabkan oleh teknologi informasi. Internet diciptakan dari teknologi informasi, media, dan komputer. Internet telah mengubah kehidupan manusia (Wahid. A & Labib. M. 2020). Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (real) ke realitas baru yang bersifat maya (virtual).

Realitas yang kedua ini biasa dikaitkan dengan internet dan cyber space. Undang-Undang Dasar 1945 memberikan kebebasan berekspresi di bawah Pasal 28 dan Pasal 28E (3) "Setiap orang berhak untuk berserikat, berkumpul, dan mengeluarkan pendapat. Sebagai warga negara, kita harus memutuskan batasan-batasan hukum, tetapi Indonesia, sebagai negara hukum, mengontrol setiap kegiatan warga negara untuk menjaga keamanan dan kenyamanan warga." Terlepas dari tujuan hukum untuk menciptakan kehidupan yang lebih damai, kejahatan tetap terjadi di sekitar kita dan di lingkungan kita baik secara langsung maupun melalui media sosial (Hasan, Z. 2020). Saat ini teknologi tidak selalu digunakan untuk kebaikan oleh masyarakat. Namun, teknologi yang terus berkembang memungkinkan para pelaku kejahatan untuk melakukan kejahatan cyber di internet atau media lainnya. Kejahatan yang berhubungan dengan komputer atau telekomunikasi disebut dengan kejahatan cyber (Akub, M.S. 2018).

Kejahatan dunia maya adalah ilegal. Kejahatan dunia maya meningkat dan membunuh banyak orang. Kejahatan dunia maya di Indonesia meliputi penipuan lelang online, pemalsuan cek, penipuan kartu kredit, penipuan kepercayaan, penipuan identitas, dan pornografi. Kasus cyber crime di Indonesia semakin berkembang sejalan dengan perkembangan internet dan teknologi yang ada. Selain karena sistem keamanan yang lemah, kasus cyber crime di Indonesia terjadi karena kelalaian yang dilakukan oleh penggunanya sendiri. Seiring dengan berkembangnya teknologi informasi, munculah satu kejahatan baru yang sedang marak terjadi di masyarakat yakni perjudian yang dilakukan secara online. Perjudian online dikategorikan sebagai cyber crime karena dalam melakukan kejahatannya, perjudian online menggunakan komputer dan internet sebagai media untuk melakukan tindak pidana perjudian tersebut. Perjudian pada dasarnya bertentangan dengan norma agama, kesusilaan, dan moral Pancasila, serta dapat membahayakan bagi keberlangsungan hidup Masyarakat, bangsa dan negara.

Perjudian merupakan pelanggaran terhadap budaya sosial di Indonesia (Hasan, Z. 2023). Sayoga mengatakan, berdasarkan data dari Pusat Pelaporan dan Analisis Transaksi Keuangan

(PPATK), sejak awal 2023 hingga saat ini total angka transaksi masyarakat Indonesia dalam judi online sudah mencapai angka Rp 200 triliun. "Angka ini cukup fantastis mengingat dari periode 2017 hingga 2022, total transaksi judi online Rp 190 triliun. Itu artinya ada lonjakan luar biasa tinggi sejak memasuki 2023 ini (Yolanda. F. 2023). Contoh lain yang pernah terjadi pada salah satu bank ternama di Indonesia, pada Mei 2023 salah satu server Bank Syariah terbesar di Indonesia dikabarkan lumpuh selama 5 hari. Menyebabkan para nasabahnya tidak dapat mengakses aplikasi mobile banking mereka. Grup hacker asal Rusia, Lockbit, mengaku bertanggung jawab atas lumpuhnya server bank tersebut. Mereka juga telah mencuri data sebesar 1,5 terabyte, termasuk di dalamnya data pribadi konsumen dan pegawai. Mereka pun mengancam pihak bank untuk membayar sejumlah uang agar data tersebut dapat dijanjikan, jika tidak maka data-data tersebut akan dijual ke dark web. Kasus cybercrime ini pun masuk ke dalam jenis serangan Ransom ware terbesar di Indonesia (6 Kasus Cybercrime Di Indonesia Yang Menyerang Server, 2023). Selain itu, sepanjang tahun 2022 terjadi banyak kasus cybercrime yang mengincar data pribadi beberapa perusahaan di Indonesia. Seperti hacker Bjorka yang sempat viral karena aksinya mencuri data pribadi milik Bank Indonesia (BI) pada awal Januari 2022. Setidaknya ada tujuh kasus besar pembobolan data yang dilakukan oleh Bjorka di tahun 2022.

Data atau informasi yang berhasil dicuri diantaranya seperti data registrasi kartu SIM milik Kominfo, data nasabah Bank Indonesia, data pasien beberapa rumah sakit di Indonesia, data pelamar Pertamina, data pelanggan PLN, data pelanggan Jasa Marga, dll. Korban pencurian data oleh Bjorka umumnya datang dari perusahaan dalam negeri dengan keamanan server yang lemah. Kasus yang lain juga yaitu pembajakan situs websit oleh serangan web deface. Web deface merupakan salah satu kasus yang banyak terjadi di Indonesia. Web deface adalah kegiatan merubah tampilan suatu website, mulai dari halaman utama, index file, atau halaman lain yang masih terikat dengan URL website tersebut. Peretas ini dapat melakukan aksi ini karena adanya celah keamanan pada sistem keamanan korban. Website yang pernah diretas adalah website yang dikelola oleh pemerintah (Popa, D.F.T. 2023)

Semakin maraknya kasus dalam teknologi tersebut mengharuskan kita lebih berhati-hati dan perlu adanya penguatan dalam hukum yang mengatur tentang hal tersebut. Oleh karena itu, pemerintah memberlakukan undang-undang yang mengatur penggunaan teknologi informasi, seperti Undang-Undang No. 19 Tahun 2016 yang mengubah Undang-Undang No. 11 Tahun 2008 yang mengatur tentang Informasi dan Transaksi Elektronik (UU ITE), untuk memberikan aturan dalam penggunaan teknologi informasi (Zainudin Hasan. 2024)

Menurut penjelasan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, hak untuk memperoleh informasi melalui penggunaan dan pemanfaatan Teknologi Informasi dan Komunikasi dimaksudkan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, serta memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan Penyelenggara Sistem Elektronik (Reyhan, R. P. 2023) Dari kasus tersebut di atas, memberikan gambaran kejadian yang timbul akibat penyalahgunaan kemajuan teknologi informasi sangat besar dampak buruknya. Oleh karena itu, diperlukan upaya-upaya pencegahan dan pemberantasan terhadap cyber crime, khususnya mengenai pengaturan hukumnya agar memberikan efek jera kepada pelaku dan calon pelaku.

Berdasarkan uraian diatas maka penitian ini berfokus pada analisis kebijakan terkait kejahatan mayantara atau cyber crime di dalam pengaturan sistem hukum positif di Indonesia.

### **Metode Penelitian**

Metode penelitian ini menggunakan pendekatan yuridis normatif dan empiris. Sumber dan jenis data yang digunakan adalah data primer dan sekunder. Pengumpulan data melalui penelitian kepustakaan. Pengolahan data dilakukan dengan menyeleksi dan memeriksa data yang diperoleh melalui kelengkapannya, serta mengklasifikasi atau mengelompokkan data secara sistematis. Analisis data yang digunakan adalah yuridis kualitatif.

### **Hasil dan Pembahasan**

Masalah cybercrime tidak dapat dilepaskan dari masalah keamanan jaringan komputer atau keamanan informasi berbasis internet di era global ini, jika dikaitkan dengan masalah informasi sebagai komoditas. Informasi sebagai sebuah komoditas membutuhkan kehandalan layanan agar apa yang disajikan tidak mengecewakan pelanggannya (Ramadhan, M. F. 2021).

Untuk mencapai tingkat kehandalan tersebut tentunya informasi harus selalu diupdate agar informasi yang disajikan tidak ketinggalan jaman. Kejahatan dunia maya ini muncul seiring dengan pesatnya perkembangan teknologi informasi. Setiap aktivitas ilegal yang melibatkan penggunaan komputer atau internet biasanya disebut sebagai kejahatan siber terkait dengan perangkat digital atau web. Aktivitas cyber yaitu kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasi sebagai orang yang melakukan perbuatan hukum secara nyata.

Namun demikian, peraturan kejahatan siber di berbagai negara menggunakan istilah yang berbeda berdasarkan tujuan dan ruang lingkup hukum mereka (Suseno, S. 2012). Menurut tipologinya, kejahatan dunia maya berasal dari kata cyber dan crime. Crime berarti kejahatan, tindak pidana, peristiwa kriminal, atau sejenisnya, sedangkan cyber berarti ruang, maya, mayantara, dunia maya (Raharjo, A. 2002).

Dalam bukunya Barda Nawawi Arief menuliskan Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapatkan perhatian luas di dunia internasional. Vodymyr Golubev menyebutnya sebagai the new form of anti-social behavior. Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (cyber space/virtual space offence) dimensi baru dari high tech crime, dimensi baru dan transnasional crime, dan dimensi baru dari white collar crime (Barda Nawawi Arief. 2018).

Dari beberapa definisi di atas, cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Berdasarkan modus atau jenis aktifitasnya cybercrime dapat digolongkan menjadi beberapa jenis yaitu sebagai berikut. Carding. Pelanggaran ini melibatkan pencurian nomor kartu kredit untuk belanja online. Setelah itu, kartu hadiah tersebut dijual untuk menghasilkan uang. Kejahatan carding melibatkan transaksi kartu kredit. Kasus kejahatan carding di dunia nyata adalah kasus

pencurian dengan lebih banyak kesulitan untuk mengidentifikasi penjahatnya. Mereka yang melakukan kejahatan carding disebut carder.

Cyber Espionage, Sabotage and Extortion. Spionase siber melibatkan penyusupan ke dalam jaringan komputer target untuk memata-matai mereka. Sabotase dan pemerasan mengganggu, merusak, atau menghancurkan data, program, atau jaringan yang terhubung ke internet. Kejahatan ini biasanya dilakukan dengan menyusupkan bom logika, virus komputer, atau program untuk mencegah data, program, atau sistem jaringan agar tidak dapat digunakan, berjalan sebagaimana mestinya, atau sesuai dengan yang diinginkan. Setelah itu, pelakunya dapat menawarkan untuk memperbaiki data, program, atau sistem jaringan yang disabotase dengan bayaran tertentu. Terorisme siber menggambarkan kejahatan ini.Cybersquatting and Typosquatting. Cybersquatting adalah kejahatan yang dilakukan dengan mendaftarkan nama domain perusahaan lain dan kemudian mencoba menjualnya ke perusahaan tersebut dengan harga yang lebih tinggi. Typosquatting adalah kejahatan yang dilakukan dengan membuat domain jiplakan, yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut adalah nama domain dari perusahaan saingannya.Cyberstalking. Kejahatan semacam ini melibatkan pelecehan berulang kali terhadap seseorang melalui komputer, seperti email. Kejahatan ini meniru teror berbasis internet. Karena membuat email dengan alamat tertentu tanpa mengungkapkan identitas asli itu mudah, hal ini bisa terjadi.

Cyber stalking melibatkan mendapatkan informasi pribadi, meneror, dan melecehkan seseorang. Cyberstalking dapat menyebabkan ketidakstabilan, trauma, dan gangguan kognitif tanpa adanya kontak fisik.Data Forgery. Kejahatan ini bertujuan untuk memalsukan dokumen-dokumen penting secara online. Organisasi dengan basis data berbasis web menyimpan dokumen-dokumen ini. Mengubah data pada dokumen penting di internet tanpa skrip merupakan sebuah kejahatan. Kejahatan ini menargetkan dokumen e-commerce dengan menggambarkannya sebagai "kesalahan ketik" untuk menguntungkan pelaku (Zainudin Hasan. 2023).

Hacking dan Cracker. Peretas sering kali tertarik untuk menganalisis sistem dan memperbaikinya. Cracker secara rutin menghancurkan internet. Bisa dibilang peretas ini adalah perusuh yang menggunakan kekuatannya untuk kejahatan. Peretasan internet dapat melibatkan pembajakan akun, situs web, menyebarkan malware, atau melumpuhkan target. Denial of Service adalah yang terakhir. Serangan DoS mencoba untuk membuat target hang atau crash sehingga tidak dapat menyediakan layanan. Hijacking Plagiarisme, atau pembajakan, adalah pencurian karya orang lain. Pembajakan perangkat lunak adalah yang paling banyak terjadi. Illegal Contens memposting informasi yang salah, tidak etis, atau ilegal secara online. Contoh: memposting berita palsu atau fitnah yang dapat merendahkan martabat atau harga diri orang lain, pornografi, rahasia negara, agitasi dan propaganda terhadap pemerintah yang sah. Ujaran kebencian kini dapat disebarluaskan secara individual melalui media sosial seperti Facebook, WhatsApp, Twitter, Instagram, dan bahkan aplikasi media sosial Gojek. Media online di mana setiap orang dapat berkontribusi dan menyebarkannya di forum dan dunia maya. Setiap orang memiliki kehadiran pribadi di media sosial dan terhubung dengan teman-teman untuk belajar dan berkomunikasi. Seiring dengan semakin mudahnya media sosial diakses, beberapa orang mulai menggunakan untuk menyebarkan ujaran kebencian terhadap etnis tertentu, seperti yang dilakukan oleh HSB Bin Yanto, seorang pengemudi ojek online (Hasan, Z., & Fadia, N. K. 2023).

Penyebaran virus secara sengaja. Email adalah vektor yang umum untuk penyebaran virus. Pengguna sistem email yang terinfeksi mungkin tidak menyadari hal ini. Malware kemudian dikirimkan ke lokasi lain melalui email. Unauthorized Access to Computer System and Service. Kejahatan yang dilakukan dengan memasuki sistem jaringan komputer secara ilegal tanpa izin atau sepengetahuan pemiliknya. Peretas biasanya mencoba mencuri atau mengganggu data sensitif.

Ada juga individu yang melakukannya karena ingin menantang diri sendiri untuk membobol sistem yang aman. Ketika isu Timor Timur sedang ramai dibicarakan di dunia internasional, para hackermeretas berbagai situs resmi Indonesia, seorang mahasiswa Fisipol ditahan karena merusak data KPU, dan masih banyak lagi contoh lainnya. Berdasarkan motif kegiatannya, cybercrime dapat digolongkan menjadi beberapa jenis diantaranya sebagai berikut: Kejahatan dunia maya murni.

Kejahatan yang murni dilakukan untuk tujuan kriminal. Kejahatan ini sering kali menggunakan internet secara eksklusif untuk melakukannya. Jenis kejahatan ini termasuk carding, yang melibatkan pencurian detail kartu kredit untuk perdagangan online. Mendistribusikan konten bajakan melalui server web, milis, dll. Kejahatan yang berhubungan dengan internet termasuk spamming.

Spam dapat dihukum karena pelanggaran privasi di berbagai negara maju. Kejahatan dunia maya itu abu-abu. Kejahatan internet di wilayah "abu-abu" sulit untuk diklasifikasikan karena motifnya terkadang bukan kejahatan. Contoh: probing atau portscanning. Ini adalah tindakan pengintaian terhadap sistem orang lain yang mengumpulkan sebanyak mungkin informasi dari sistem yang dipantau, seperti sistem operasi, port yang terbuka dan tertutup, dll (Suhaemin, A., & Muslih, M. 2023).

Hak dan kebebasan dalam masyarakat demokratis, termasuk yang terkait dengan teknologi informasi, harus dilaksanakan dalam batas-batas yang ditetapkan oleh hukum sehingga hak dan kebebasan setiap orang diakui dan dihormati, dan agar tuntutan yang adil dari setiap orang dapat dipenuhi dengan cara yang sesuai dengan prinsip-prinsip moral, keyakinan agama, keamanan publik, dan ketertiban umum. Dalam konteks ini, "informasi elektronik" mengacu pada setiap data yang telah diolah, baik berupa teks, audio, gambar, peta, rancangan, foto, EDI, surat elektronik, telegram, teleks, telecopy, atau sejenisnya, huruf, angka, Kode Akses, simbol, atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh manusia.

Peraturan kejahatan siber didasarkan pada sumber hukum terkini, termasuk KUHP dan undang-undang lainnya. Kitab Undang-Undang Hukum Pidana (KUHP) Pasal-pasal di dalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada cyber crime. Pengaturan bentuk cyber crime di dalam KUHP dapat dilihat pada pasal-pasal sebagai berikut: (Jannah, H. S., & Naufal, M. 2012)

- a. Pasal 282 KUHP tentang kejahatan terhadap kesopanan; Distribusi pornografi dapat dibatasi meskipun dalam bahasa Indonesia, para penjahat mendaftarkan domain di luar negeri, di mana pornografi dewasa diizinkan, sehingga lebih sulit untuk dituntut. Penyebar foto-foto vulgar atau video pribadi di Internet dapat dikenai hukuman. Video porno pelajar, pekerja, dan pejabat publik di Internet.
- b. Pasal 303 KUHP tentang Perjudian; dapat diterapkan pada permainan judi internet yang diselenggarakan oleh orang Indonesia. Di dalamnya mengatur tentang pelanggaran perjudian. Pasal tersebut membahas hukuman perjudian.

- c. Pasal 311 KUHP tentang Pencemaran nama baik; Hukuman pencemaran nama baik melalui media internet dapat diajukan. Pelaku mengirim email kepada teman-teman korban atau milis dengan cerita palsu.
- d. Pasal 335 KUHP berkaitan dengan perbuatan tidak menyenangkan, khususnya mengenai kejahatan terhadap kemerdekaan orang. Pasal 335 KUHP berisi sanksi atau hukuman bagi para pelaku yang telah melakukan pemaksaan terhadap orang lain. Dapat diterapkan pada ancaman dan Penjahat mengirimkan email untuk memeras korban, yang mungkin memiliki konsekuensi serius jika tidak dilakukan. Hal ini sering dilakukan ketika pelaku mengetahui rahasia korban.
- e. Pasal 362 KUHP tentang pencurian; Pelaku bertanggung jawab dalam kasus carding, di mana nomor kartu kredit korban digunakan untuk melakukan pembelian online tanpa benar-benar memiliki kartu itu sendiri. Setelah transaksi selesai dan produk telah dikirim, penjual mencoba menarik dana dari bank, tetapi ditolak karena pemegang kartu bukan orang yang sama dengan yang melakukan pembelian. Orang yang melakukan pembelian tidak memiliki kartu tersebut.
- f. Pasal 378 KUHP tentang penipuan; Anda dapat dituntut dengan tuduhan penipuan jika Anda diduga menjual produk atau layanan dengan memasang iklan di situs web untuk menarik minat dan pembayaran. Mengirimkan uang kepada pengiklan. Kenyataannya, barang yang dijual tidak ada. Setelah membayar barang yang tidak kunjung tiba, pembeli tertipu.
- g. Pasal 406 KUHP tentang Pengrusakan; Hukuman dapat diberlakukan untuk defacing atau peretasan yang mengganggu sistem orang lain, seperti situs web atau program. Undang-Undang No. 19 Tahun 2016 yang mengubah Undang-Undang No. 11 Tahun 2008 yang mengatur tentang Informasi dan Transaksi Elektronik (UU ITE) Dengan semakin berkembangnya kebutuhan akan peraturan perundang-undangan pidana, khususnya dalam kejahatan mayantara, yang tidak diatur dalam KUHP sebagai acuan dalam mengatur kebijakan kejahatan mayantara, maka disahkanlah UU No. 11 Tahun 2008 yang dirubah dengan UU No. 19 Tahun 2016 tentang Informasi Transaksi Elektronik (ITE), Undang-Undang ini mengatur kejahatan mayantara untuk pertama kalinya. Khususnya dalam Pasal 27 sampai dengan Pasal 37 tentang Perbuatan yang dilarang dan dalam Pasal 45 sampai dengan Pasal 52 tentang ancaman penjara dengan mengenakan ancaman hukuman penjara paling berat 12 (dua belas) tahun dan hukuman denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

Dengan demikian, UU No. 19/2016 adalah cara yang tepat untuk mempromosikan etika media. Penjelasan Umum paragraf kesembilan UU No. 19/2016, yang menetapkan undang-undang ini untuk mempromosikan etika media, menyatakan bahwa "... virtualitas dunia maya memungkinkan adanya konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang melanggar kesuilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan, dan penyebaran informasi yang tidak benar dan menyesatkan."

Pemerintah harus memperkuat perannya dalam mencegah penyebaran konten ilegal dengan cara melakukan pemblokiran terhadap akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang isinya melanggar hukum untuk melindungi kepentingan umum. Pengadilan dan penyidik di Indonesia harus dapat memperoleh informasi penyelenggara sistem elektronik untuk penegakan hukum tindak pidana informasi dan transaksi elektronik.

## Kesimpulan

Berdasarkan hasil kajian dan analisis normatif menunjukkan bahwa Teknologi Informasi dan Komunikasi (TIK) mempengaruhi peraturan perundang-undangan dan budaya masyarakat. Teknologi informasi bisa berdampak baik dan buruk, seperti kejahatan siber. Kejahatan siber tumbuh dengan teknologi informasi, sehingga menyulitkan pengaturannya. Peradaban manusia telah menciptakan banyak masalah baru. Perkembangan manusia menciptakan masalah baru seperti kejahatan elektronik. Semua tindakan di Indonesia harus mengikuti hukum karena Indonesia adalah negara hukum. Kejahatan dunia maya dapat diklasifikasikan berdasarkan: 1) modus atau jenis kegiatan, seperti Carding; Cyber Espionage, Sabotage and Extortion; Cybersquatting and Typosquatting; Cyberstalking; Data Forgery; Hacking dan Cracker; Hijacking; Illegal Contests; Penyebaran virus secara sengaja; Unauthorized Access to Computer System and Service; dan 2) motif, seperti kejahatan murni atau kejahatan abu-abu. Dari hasil analisis di atas juga menunjukkan bahwa setidaknya ada 7 Peraturan Perundang-Undangan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Republik Indonesia, khususnya Undang-Undang No. 19 Tahun 2016 yang merupakan amandemen dari Undang-Undang No. 11 Tahun 2008, yang mengatur tentang kejahatan siber di Indonesia.

## **Daftar Pustaka**

- Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *Al-Ishlah: Jurnal Ilmiah Hukum*. Vol. 21. No. 2.
- Barda Nawawi Arief, S. H. (2018). Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan. *Kencana Prenada Media Group*.
- Hasan, Z., Apriano, I. D., Simatupang, Y. S., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. *Jurnal Multidisiplin Dehasen (MUDE)*. Vol. 2. No.3.
- Hasan, Z., & Fadia, N. K. (2023). Pertanggung Jawaban Pelaku Tindak Pidana Dengan Sengaja Menyebarluaskan Informasi Yang Ditunjukan Untuk Menimbulkan Rasa Kebencian Atau Permusuhan Individu Dan Kelompok Masyarakat Tertentu Berdasarkan Sara. *UNES Law Review*. Vol. 5. No. 3.
- Hasan, Z., & Martinouva, R. A. (2020). Penanggulangan Kejahatan Begal Di Tulang Bawang Barat (Dalam Perspektif Kriminologi). *Jurnal Hukum Malahayati*. Vol. 1. No. 1.
- Jannah, H. S., & Naufal, M. (2012). Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam. *Jurnal Al-Mawarid*, 12(1), 70–84. Kementerian Komunikasi dan Informasi RI. (n.d.). Pasal 5 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).
- Popal, D. F. T. (2023). Upaya Penanggulangan Tindak Pidana Mayantara (CyberCrime). *Lex Administratum*. Vol. 11. No. 5.
- Raharjo, A. (2002). Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi. *Citra Aditya Bakti*.
- Ramadhan, M. F. (2021). Analisis Hukum Terhadap Penyebaran Berita Bohong/Hoax sebagai Bentuk Cyber Crime di Indonesia (Studi Putusan No. 3478/Pid. Sus/2019/Pn. Mdn). *Universitas Medan Area*.
- Reyhan, R. P., Irfan, M., Alfido, M. T. B., & Zai, M. C. A. (2023). Pengaturan Tindak Pidana Elektronik Di Indonesia Beserta Permasalahannya. *Innovative: Journal Of Social Science Research*. Vol. 3. No. 2.
- Soerjono, S., & Mamudji, S. (1986). *Pengantar Penelitian Hukum*, Jakarta. UI Press.

- Suhaemin, A., & Muslih, M. (2023).Karakteristik Cybercrime di Indonesia. Edulaw: Journal of Islamic Law and Jurisprudence. Vol. 5. No. 2.
- Suseno, S. (2012). Yurisdiksi Tindak Pidana Siber. Refika Aditama.
- Wahid, A., & Labib, M. (2010). Kejahatan Mayatantra (Cyber Crime). Bandung: Refika Aditama.
- Yolandha, F., & Subekti, R. (2023). Judi Online Marak di Kalangan Pelajar, Bukti Literasi Masyarakat Rendah. Jurnal Republika. Vol. 3. No. 1.
- Zainudin Hasan. 2023. *Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online*. Jurnal Multi Disiplin Dehasen. Vol. 2. No. 3.
- Zainudin Hasan. 2024. *Kejahatan Mayantara. Berupa Tindak Pidana Perjudian Melalui Media Elektronik*. Journal Innovative: Journal of Social Science Research. Vol. 4 No. 1.