Jurnal Thengkyang
Volume 9 (2), 2024: 80 - 86
E-ISSN: 2655-1810 | P-ISSN: 2541-3813

Pengaturan Tindak Pidana Mayantara (*Cyber Crime*) dalam Sistem Hukum Indonesia

Waliadin
Universitas Sjakyahkirti Palembang
E-mail: waliadin@unisti.ac.id

Abstract

The development of information technology driven by globalization has had significant positive and negative impacts on society. One negative impact that has emerged is the increase in cybercrime cases, which has become a global concern, including in Indonesia. This study aims to analyze the regulation of cybercrime offenses within the Indonesian legal system, focusing on the implementation of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions (UU ITE) and the Indonesian Penal Code (KUHP). This research employs a normative method by analyzing legal texts, doctrines, and related cases. The findings indicate that although regulations related to cybercrime are in place, their implementation faces several obstacles, highlighting the need for strengthened regulations and the expedited enactment of the Cyberlaw Bill to provide more effective legal protection for society in the digital era.

Keywords: *Information Technology, Globalization, Cybercrime, ITE Law, KUHP, Cyberlaw Bill*

Abstrak

Perkembangan teknologi informasi yang dipicu oleh globalisasi telah membawa dampak signifikan baik positif maupun negatif terhadap kehidupan masyarakat. Salah satu dampak negatif yang muncul adalah peningkatan kasus kejahatan mayantara atau cybercrime, yang menjadi perhatian global, termasuk di Indonesia. Penelitian ini bertujuan untuk menganalisis pengaturan tindak pidana cybercrime dalam sistem hukum Indonesia, dengan fokus pada implementasi Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP). Penelitian ini menggunakan metode normatif dengan menganalisis teks-teks hukum, doktrin, dan kasus-kasus terkait. Hasil kajian menunjukkan bahwa meskipun regulasi terkait cybercrime telah ada, implementasinya masih menghadapi berbagai hambatan, sehingga diperlukan penguatan regulasi dan percepatan pengesahan RUU Cyberlaw untuk memberikan perlindungan hukum yang lebih efektif bagi masyarakat di era digital ini.

Kata kunci: Teknologi Informasi, Globalisasi, Cybercrime, UU ITE, KUHP, RUU Cyberlaw

PENDAHULUAN

Perkembangan teknologi informasi dipicu oleh globalisasi. Fenomena perkembangan teknologi informasi yang cepat di era modern ini telah menyebar di seluruh dunia. Teknologi informasi sangat penting untuk kemajuan negara, baik di negara maju maupun berkembang (Rachman Ma'ruf et al., 2023). Teknologi yang berkembang sangat pesat memiliki banyak

Universitas Sjakyahkirti Palembang
Waliadin
*E-mail: waliadin@unisti.ac.id

efek positif dan negatif terhadap kehidupan manusia. Salah satu faktor yang mendorong kemajuan teknologi yang tak terbatas adalah globalisasi. Pengetahuan muncul sebagai hasil dari perkembangan daya fikir. Tidak semua orang dapat memanfaatkan pengetahuan ini dengan bijak dan benar, sehingga sangat merugikan banyak orang. Sebagai contoh, pelanggaran yang melibatkan sistem atau jaringan komputer dan sarana computer (Arief, 2006).

Salah satu jenis kejahatan mayatara atau *cybercrime* yang muncul sebagai akibat dari kemajuan teknologi ialah tindak pidana peretasan. Dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UUITE), pasal 30 ayat (1), (2), dan (3) mengatur hal ini. Pasal 46 UUITE juga mengatur sanksi pidananya. Teknologi tidak hanya bermanfaat, tetapi juga berbahaya bagi masyarakat (Noval et al., 2022).

Semua negara menghadapi peningkatan kasus *cybercrime*. Pada Kongres PBB ke-8 tahun 1990 di Havana, Kuba dan Kongres ke-10 tahun 1990 di Wina, Austria, *cybercrime* menjadi salah satu topik diskusi. Karena banyaknya aktivitas hacker di Tanah Air, Indonesia memiliki kasus *cybercrime* tertinggi di dunia. *Cybercrime* terhadap anak disebutkan telah menjadi tren baru di banyak negara, termasuk Indonesia.Penggunaan internet yang hampir tidak terkendali meningkatkan kemungkinan anak-anak menjadi korban berbagai tindak kejahatan online. Kejahatan yang dilakukan secara online, termasuk kejahatan seksual, pornografi, *trafficking*, *bullying*, dan jenis kejahatan lainnya, semakin mengancam generasi muda negara ini (Akub, 2020).

Karena banyaknya aktivitas *hacker* di Tanah Air, Indonesia memiliki kasus *cybercrime* tertinggi di dunia. *Cybercrime* terhadap anak disebutkan telah menjadi tren baru di banyak negara, termasuk Indonesia. Penggunaan internet yang hampir tidak terkendali meningkatkan kemungkinan anak-anak menjadi korban berbagai tindak kejahatan online. Kejahatan yang dilakukan secara online, termasuk kejahatan seksual, pornografi, *trafficking*, *bullying*, dan jenis kejahatan lainnya, semakin mengancam generasi muda negara ini (Simon Nahak, 2017). Selain itu, memastikan bahwa pelaku dapat bertanggung jawab atas tindakannya sehingga kejahatan *cyber* dapat dicegah melalui hukum pidana, termasuk sistem pembuktian (Surbakti, 2005).

Cybercrime dapat terjadi di mana saja dan kapan saja tanpa ada interaksi langsung antara pelaku dan korbannya. Dengan kenyataan bahwa internet tersebar di seluruh dunia, hampir pasti perkem-bangan kejahatan internet ini akan terjadi di negara mana pun yang melakukan

http://jurnal.unisti.ac.id/thengkyang/index
E-ISSN: 2655-1810 | P-ISSN: 2541-3813

aktivitas internet. Saat ini, Undang-undang Telekomunikasi Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana (KUHP) digunakan sebagai dasar hukum untuk kasus *cybercrime*. Namun demikian, interpretasi pasal-pasal KUHP dalam kasus *cybercrime* terkadang tidak tepat. Oleh karena itu, untuk menghadapi era internet dan segala konsekuensi yang menyertainya, termasuk peningkatan kejahatan internet belakangan ini, pengesahan RUU *Cyberlaw* harus menjadi prioritas utama.

Rumusan masalah dalam konteks perkembangan teknologi informasi yang dipicu oleh globalisasi mencakup bagaimana globalisasi telah mendorong kemajuan teknologi yang pesat. Hal ini berdampak baik secara positif maupun negatif terhadap masyarakat, termasuk munculnya berbagai bentuk *cybercrime* seperti tindak pidana peretasan dan kejahatan online terhadap anak-anak di Indonesia. Pertanyaannya adalah, bagaimana pengaturan tindak pidana mayantara (*cybercrime*) dalam sistem hukum Indonesia?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian normatif, di mana fokus utama adalah pada kajian terhadap peraturan perundang-undangan yang relevan, seperti Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), dalam konteks penanganan kasus *cybercrime* di Indonesia. Metode ini melibatkan analisis terhadap teks hukum, doktrin hukum, dan kasus-kasus yang terkait untuk memahami bagaimana regulasi yang ada diterapkan serta mengidentifikasi kelemahan dan kekurangan hukum dalam menghadapi perkembangan teknologi informasi dan *cybercrime*. Data yang digunakan bersumber dari bahan hukum primer, sekunder, dan tersier yang dikaji secara mendalam untuk memberikan gambaran mengenai efektivitas regulasi hukum yang ada serta kebutuhan akan pengesahan RUU *Cyberlaw* di Indonesia.

HASIL DAN PEMBAHASAN

Kejahatan siber (*cybercrime*) yang muncul sebagai akibat dari pesatnya kemajuan teknologi telah membawa dampak baik negatif maupun positif bagi masyarakat. Teknologi yang berkembang dengan cepat memang menawarkan berbagai manfaat, namun di sisi lain juga memunculkan berbagai ancaman baru, termasuk kejahatan digital yang dapat merugikan individu dan masyarakat luas (Soedjono Dirjosisworo, 2002). Dampak positif dari perkembangan teknologi ini meliputi kemudahan dalam penggunaan e-mail, layanan perbankan online, dan berbagai inovasi lainnya. Namun, kemajuan tersebut juga membawa

E-ISSN: 2655-1810 | P-ISSN: 2541-3813

dampak negatif, seperti munculnya tindak kejahatan peretasan (*hacking*) yang bertujuan untuk mendapatkan informasi atau data-data penting (Singgi et al., 2020).

Tindakan ini dilakukan tidak hanya untuk mencari keuntungan dan mengidentifikasi kelemahan target. Kejahatan ini relatif baru jika dibandingkan dengan kejahatan konvensional lainnya. Meskipun jenis kejahatan ini sudah muncul sejak tahun 1961, kejahatan ini tidak sepopuler kejahatan konvensional yang lebih dikenal oleh masyarakat. Meskipun telah ada sejak lama, belum ada kesepakatan di antara para ahli mengenai definisi yang tepat untuk kejahatan siber (*cybercrime*) maupun tindak pidana peretasan itu sendiri. Namun demikian, berbagai istilah seperti siber, kejahatan dunia maya, kejahatan virtual, dan tetap menggunakan istilah *cybercrime* sudah banyak digunakan.

Cybercrime adalah kegiatan kejahatan yang dilakukan di dunia maya dengan memanfaatkan jaringan komputer sebagai perangkatnya dan jaringan internet sebagai medianya. Dalam makna yang luas, *cybercrime* mencakup semua tindakan ilegal yang dilakukan melalui jaringan komputer dan internet untuk mendapatkan keuntungan dengan merugikan pihak lain. Dalam makna yang lebih sempit, *cybercrime* adalah semua tindakan ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh sistem komputer.

Cybercrime sendiri memiliki sejarah yang cukup panjang. Jadi, kegiatan ini pertama kali dimulai dengan peretas yang mencoba membobol jaringan komputer. Beberapa melakukannya hanya untuk sensasi mengakses jaringan keamanan tingkat tinggi, tetapi yang lain berusaha untuk mendapatkan materi rahasia yang sensitif. Akhirnya, penjahat mulai menginfeksi sistem komputer dengan virus komputer, yang menyebabkan kerusakan pada komputer pribadi dan bisnis. Kesulitan menanggulangi kejahatan tersebut karena disebabkan oleh kurang tersedianya peralatan yang memadai, keengganan dari beberapa korban untuk melapor kepada polisi, sistem keamanan dari pemilik aset/sistem yang relatif lemah, sulit melacak keberadaan/domisili pelaku kejahatan (Musa Sahat Tobing et al., 2023).

Virus komputer adalah bentuk kode atau program malware yang dapat menyalin dirinya sendiri dan merusak atau menghancurkan data dan sistem. Ketika virus komputer digunakan dalam skala besar, seperti jaringan bank, pemerintah, atau rumah sakit, tindakan ini dapat dikategorikan sebagai terorisme siber. Peretas komputer juga terlibat dalam penipuan phishing, seperti meminta nomor rekening bank, dan pencurian kartu kredit. Namun pada puncaknya, akhirnya di tahun 1996 Dewan Eropa, bersama dengan perwakilan pemerintah dari Amerika Serikat, Kanada, dan Jepang, merancang perjanjian internasional

http://jurnal.unisti.ac.id/thengkyang/index
E-ISSN: 2655-1810 | P-ISSN: 2541-3813

awal yang mencakup kejahatan komputer. Di seluruh dunia, kelompok libertarian sipil segera memprotes ketentuan dalam perjanjian yang mengharuskan seluruh Internet Service Provider untuk menyimpan informasi tentang transaksi pelanggan mereka dan menyerahkan informasi ini sesuai permintaan. Konverensi tersebut akhirnya bisa ditandatangani oleh 30 negara dan selesai pada tahun 2001 dan mulai berlaku pada tahun 2004.

Pengaturan Mayantara (*cybercrime*) melalui Hukum Pidana

Pada era modern ini, kemajuan teknologi informasi telah memicu peningkatan kasus kejahatan mayantara atau *cybercrime*, yang menimbulkan keresahan di kalangan masyarakat, terutama bagi mereka yang bergantung pada komputer dan teknologi informasi. Menyadari urgensi masalah ini, Kongres PBB telah mengimbau negara-negara anggotanya untuk menanggulangi *cybercrime* melalui sarana penal. Meskipun implementasinya tidak mudah, perlindungan hukum bagi para korban kejahatan siber menjadi kebutuhan mendesak yang harus segera diakomodasi oleh negara. Pengaturan hukum terkait *cybercrime* di Indonesia didasarkan pada sumber hukum yang berlaku saat ini, baik dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun undang-undang lain di luar KUHP (Rizky, 2023).

Dalam KUHP, beberapa pasal yang terkait dengan bentuk-bentuk *cybercrime* antara lain Pasal 362 tentang pencurian, Pasal 369 tentang pemerasan dan pengancaman, Pasal 372 tentang penggelapan, dan Pasal 386 tentang perbuatan curang. Selain itu, pengaturan yang lebih spesifik terkait *cybercrime* dapat ditemukan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur berbagai bentuk kejahatan siber, seperti konten ilegal (Pasal 27 dan Pasal 28), akses ilegal (Pasal 30), penyadapan ilegal (Pasal 31), kebocoran data dan spionase (Pasal 32), interferensi sistem (Pasal 33), penyalahgunaan perangkat (Pasal 34), dan gangguan data (Pasal 35).

Pasal-pasal dalam UU ITE ini mencakup berbagai tindakan yang dianggap melanggar hukum di dunia maya, mulai dari penyebaran konten pornografi dan berita palsu, hingga peretasan sistem elektronik dan manipulasi data. Meskipun peraturan ini telah ada, keefektifan dan implementasinya masih menjadi tantangan besar dalam menghadapi kejahatan siber yang terus berkembang. Hal ini menegaskan pentingnya penguatan regulasi dan penegakan hukum untuk melindungi masyarakat dari ancaman *cybercrime*.

KESIMPULAN

Perkembangan teknologi informasi yang pesat akibat globalisasi telah membawa dampak yang signifikan, baik positif maupun negatif, terhadap masyarakat. Meskipun teknologi informasi menawarkan berbagai kemudahan, seperti email dan internet banking,

http://jurnal.unisti.ac.id/thengkyang/index
E-ISSN: 2655-1810 | P-ISSN: 2541-3813

kemajuan ini juga memunculkan ancaman baru berupa kejahatan siber (*cybercrime*), termasuk tindak pidana peretasan. Indonesia, seperti banyak negara lain, menghadapi tantangan serius dalam menangani *cybercrime*, terutama mengingat dampak buruknya terhadap masyarakat, khususnya anak-anak. Meskipun terdapat peraturan dalam KUHP dan UU ITE yang mengatur berbagai bentuk kejahatan siber, implementasinya sering kali menghadapi hambatan, seperti kurangnya alat yang memadai dan kerentanan sistem keamanan. Oleh karena itu, penting bagi negara untuk memperkuat regulasi dan penegakan hukum, serta mempercepat pengesahan RUU *Cyberlaw* guna memberikan perlindungan hukum yang efektif bagi masyarakat di era digital ini.

DAFTAR PUSTAKA

Akub, M. S. (2020). Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia. *Al-Ishlah : Jurnal Ilmiah Hukum*, *21*(2), 85–93. https://doi.org/10.33096/aijih.v20i2.19

Arief, B. N. (2006). *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*. Rajawali Pers.

Musa Sahat Tobing, Utari Wulandari, Marito Sari Sihotang, & Raihana Raihana. (2023). Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime. *Jurnal Hukum Dan Sosial Politik*, *1*(2), 60–67. https://doi.org/10.59581/jhsp-widyakarya.v1i2.239

Noval, M., Nofrial, R., & Nurkhotijah, S. (2022). Analisis Yuridis Proses Penyelesaian Tindak Pidana Terhadap Pelaku Penipuan Melalui Pembayaran Elektronik Untuk Mewujudkan Perlindungan Hukum. *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia*, *2*(1), 29–37. https://doi.org/10.35912/jihham.v2i1.1579

Rachman Ma'ruf, Indra Lamhot Sihombing, Fradhil Mensa, & Raihana Raihana. (2023). Pengaturan Hukum Tindak Pidana Penipuan Secara Online Dalam Perspektif Hukum Pidana di Indonesia. *Jurnal Hukum Dan Sosial Politik*, *1*(2), 10–20. https://doi.org/10.59581/jhsp-widyakarya.v1i2.207

Rizky, M. (2023). Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations. *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *12*(1), 120. https://doi.org/10.20961/recidive.v12i1.69292

Simon Nahak. (2017). *Hukum Tindak Pidana Mayantara (Cyber Crime) Dalam Perspektif Akademik*. *4*(1), 37–49. https://doi.org/10.22225/jhp.4.1.161.1-11

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), 334–339. https://doi.org/10.22225/jkh.2.1.2553.334-339

Soedjono Dirjosisworo. (2002). *Respon Terhadap Kejahatan,Introduksi Hukum Penanggulangan Kejahatan(Introduction to The Law of Crime Prevention)*. STHB Press.

Surbakti, S. dan N. (2005). *Hukum Pidana*. Fakultas Hukum UMS.