

MEMERANGI KEJAHATAN SIBER DI INDONESIA: ANALISIS REGULASI HUKUM PIDANA YANG BERLAKU DAN TANTANGANNYA

Andi Mohammad Agus Mustam
Magister Hukum Universitas Islam Batik Surakarta
E-mail : ddmk@rocketmail.com

ABSTRAK

The rapid development of information technology and digitalization in various aspects of life has not only brought positive impacts but has also given rise to a new phenomenon called cybercrime. Cybercrime is a type of criminal activity that involves the use of digital technology and the internet. Cybercrime covers a wide range of offenses, from illegal access to computer systems, theft of data and information, the spread of malware, online fraud, defamation, to violations of personal data privacy. The surge in cybercrime cases in Indonesia calls for an urgent evaluation of the current criminal law regulations. This literature review aims to examine and analyze the laws and regulations in Indonesia related to criminal offenses in cyberspace and the extent of their effective implementation. The primary regulations that are the focus of the analysis include the Electronic Information and Transactions Law along with its amendments, as well as the latest 2019 Draft Criminal Code that contains new provisions on cybercrime.

ARTICLE INFO

Article History:

Accepted 03 Juni 2023

Available online 30 Jul 2023

Kata kunci: *cybercrime, criminal law, Electronic Information and Transactions Law (ITE Law), Draft Criminal Code (RKUHP)*

I. PENDAHULUAN

Indonesia, dengan populasi lebih dari 270 juta jiwa dan pertumbuhan internet yang cepat, menjadi sasaran empuk bagi para penjahat siber. Serangan siber meliputi beragam aktivitas, mulai dari pencurian data pribadi, penipuan online, hingga serangan terhadap infrastruktur kritis negara.

Salah satu tantangan utama dalam memerangi kejahatan siber adalah tingkat kesadaran masyarakat. Banyak individu dan organisasi yang kurang memahami ancaman yang dihadapi dan cara untuk melindungi diri dari serangan tersebut. Selain itu, kurangnya kerjasama antara sektor publik dan swasta juga menjadi masalah serius. Keterbatasan sumber daya dan keahlian teknis yang diperlukan untuk melacak dan menanggapi

serangan siber menjadi hambatan dalam membangun kapasitas yang diperlukan.

Indonesia telah mengeluarkan sejumlah undang-undang untuk mengatasi kejahatan siber. Undang-undang ITE (Informasi dan Transaksi Elektronik) adalah salah satu regulasi utama yang digunakan untuk menangani kejahatan siber. Namun, implementasi undang-undang ini sering menimbulkan kontroversi dan kritik karena dianggap ambigu dan berpotensi menekan kebebasan berbicara. Selain Undang-Undang ITE, terdapat juga regulasi lain yang relevan, seperti Undang-Undang Perlindungan Data Pribadi dan Peraturan Bank Indonesia tentang Keamanan Informasi. Namun, masih terdapat celah hukum dan kekurangan dalam kerangka regulasi yang ada. Misalnya, kurangnya

ketentuan yang jelas mengenai penegakan hukum terhadap pelaku kejahatan siber, serta kurangnya sanksi yang memadai untuk pelanggaran keamanan cyber. Tantangan utama dalam memerangi kejahatan siber di Indonesia meliputi:

Keterbatasan Sumber Daya: Keterbatasan dana, tenaga kerja, dan infrastruktur merupakan hambatan utama dalam membangun kapasitas untuk menangani kejahatan siber. **Kesadaran Masyarakat:** Kurangnya kesadaran masyarakat tentang risiko kejahatan siber dan cara melindungi diri mereka sendiri merupakan tantangan serius. Pendidikan dan sosialisasi tentang keamanan cyber perlu ditingkatkan.

Kerjasama Antar-lembaga: Koordinasi dan kerjasama antara lembaga pemerintah, sektor swasta, dan masyarakat sipil perlu ditingkatkan untuk mengatasi kejahatan siber secara efektif. **Perubahan Teknologi:** Kecepatan perkembangan teknologi menyulitkan untuk membuat regulasi yang relevan dan efektif dalam jangka panjang.

Aspek Internasional: Kejahatan siber sering kali lintas batas, sehingga kerjasama internasional menjadi penting. Namun, perbedaan dalam regulasi dan hukum antarnegara dapat menjadi hambatan dalam penegakan hukum.

Kejahatan siber di Indonesia terus menunjukkan peningkatan dari tahun ke tahun. Menurut data dari Direktorat Tindak Pidana Siber Bareskrim Polri, pada tahun 2021 terdapat 7.921 kasus kejahatan siber yang dilaporkan dan ditangani. Angka ini meningkat signifikan sekitar 400% apabila dibandingkan dengan jumlah kasus pada tahun sebelumnya. Kenaikan kasus yang sangat drastis ini menunjukkan makin maraknya kejahatan dunia maya seiring perkembangan teknologi dan transformasi digital di berbagai sektor. Kejahatan siber yang paling banyak dilaporkan yaitu penipuan online, pencurian data pribadi, pencemaran nama baik, dan pemalsuan identitas di internet (Butarbutar, 2023).

Tren peningkatan ini mendorong urgensi regulasi hukum pidana khusus yang

mampu menangani kejahatan siber (Farhan et al., 2023). Diperlukan rumusan pasal-pasal pidana yang tegas dan rinci untuk mencegah celah hukum serta menjamin proses penegakan hukum yang efektif dalam menghadapi kejahatan era digital. Selain itu, sanksi pidana juga harus memadai agar memberi efek jera bagi pelaku. Regulasi yang ada saat ini, seperti UU ITE dan perubahannya, dinilai masih terlalu umum dan belum mampu mengikuti perkembangan modus operandi kejahatan siber yang makin canggih. Oleh karena itu sangat dibutuhkan penyesuaian regulasi yang terukur dan antisipatif terhadap trend teknologi informasi ke depan agar dapat memberantas kejahatan siber yang terus meningkat dari tahun ke tahun tersebut

II. METODE PENELITIAN

Jenis penelitian yang digunakan dalam penulisan jurnal ilmiah ini adalah jenis penelitian hukum yuridis normatif, yaitu penelitian hukum yang meletakkan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud adalah mengenai asas-asas, norma, kaidah dari peraturan perundang-undangan, putusan pengadilan, perjanjian serta doktrin. Dalam menunjang proses penelitian jenis pendekatan yang digunakan ialah pendekatan perundang-undangan yang dilakukan dengan melihat undang-undang dan regulasi yang bersangkutan dengan rumusan masalah dan pendekatan konseptual. Bahan hukum yang digunakan dalam penulisan jurnal ini adalah bahan hukum primer berupa peraturan perundang-undangan yaitu Kitab Undang-Undang Hukum Pidana dan Undang-undang No 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selanjutnya, bahan hukum sekunder juga digunakan yaitu berupa buku-buku, jurnal ilmiah dan literature lain yang menunjang

tulisan ini. Teknik pengumpulan bahan hukum yaitu teknik kepustakaan.

III. HASIL PENELITIAN DAN PEMBAHASAN

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah hukum yang berlaku di Indonesia yang mengatur tentang informasi dan transaksi elektronik (Parulian & Putranto, 2022). Berikut ini adalah beberapa hal penting yang diatur dalam UU ITE:

- a. **Pasal 27** berisi tentang tindak pidana akses ilegal ke dalam sistem elektronik. Pelaku dapat dihukum dengan pidana penjara paling lama 6 tahun dan/atau denda hingga Rp 600.000.000.
- b. **Pasal 28** mengatur tentang tindak pidana intersepsi ilegal terhadap informasi elektronik dan/atau dokumen elektronik. Ancaman hukumannya bisa mencapai 10 tahun penjara dan/atau denda hingga Rp 800.000.000.
- c. **Pasal 29** adalah tentang akses komputer dengan tujuan ilegal seperti manipulasi, pencurian, penghilangan, perusakan, atau pemalsuan dokumen. Ancaman hukumannya adalah penjara antara 3 hingga 12 tahun, dan/atau denda mulai dari Rp 600 juta sampai Rp 2 miliar.
- d. **Pasal 30 dan 31** mengatur tentang penyebaran konten ilegal seperti perjudian, SARA (pencemaran nama baik), berita palsu dan lain sebagainya. Ancaman hukumannya bisa mencapai 6 hingga 12 tahun penjara dan/atau denda mulai dari Rp1 miliar hingga Rp2 miliar.
- e. **Pasal 32 hingga 37** mencakup berbagai tindak pidana lainnya yang terkait dengan teknologi informasi dan transaksi elektronik.

Meski secara komprehensif UU ITE telah mengatur jenis tindak pidana siber dan ancaman hukumannya, namun kritik yang muncul adalah batasan pengertian untuk masing-masing tindak pidana yang masih terlalu umum, sehingga rawan terjadi penafsiran ganda dalam penerapannya.

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU No.11/2008

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU No.11/2008 (UU ITE) bertujuan untuk menjawab tantangan perkembangan kejahatan siber dan memperbaharui aturan yang ada (Supanto et al., 2023). Berikut adalah beberapa perubahan penting dalam UU ini:

- a. **Memperluas subjek hukum:** UU 19/2016 memperluas subjek hukum yang dapat dihukum, meliputi perseorangan, korporasi (badan hukum), dan/atau penyelenggara negara. Hal ini memberikan cakupan yang lebih luas dalam penegakan hukum terhadap kejahatan siber.
- b. **Penambahan jenis tindak pidana siber:** UU ini menambahkan 2 pasal baru, yaitu Pasal 45A yang mengatur tentang tindak pidana penyalahgunaan sarana teknologi informasi untuk melakukan kejahatan dan Pasal 45B yang mengatur tentang tindak pidana pengancaman, pemerasan, atau penyebaran konten yang mengganggu ketertiban umum melalui teknologi informasi.
- c. **Perubahan Pasal 27 ayat (3) dan Pasal 45:** Pasal 27 ayat (3) yang mengatur illegal access mengalami perubahan dengan ditambahkannya frasa "tanpa hak" sebelum "mengakses Komputer dan/atau Sistem Elektronik milik Orang lain". Sementara itu, Pasal 45 mengalami perubahan ancaman pidana menjadi maksimal 8 tahun penjara dan/atau denda paling banyak Rp2 miliar dari sebelumnya 6 tahun penjara (Nuralifa, 2023).

Diharapkan dengan perubahan yang ada dalam UU 19/2016, penegakan hukum terhadap kejahatan siber di Indonesia akan menjadi lebih efektif. Namun demikian, penerapannya di lapangan masih sering menimbulkan multitafsir dan polemik dalam masyarakat. Oleh karena itu, diperlukan pemahaman yang komprehensif dan penerapan yang bijaksana untuk memastikan keadilan dan kepastian hukum bagi masyarakat.

3. Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) Tahun 2019

Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) tahun 2019 merupakan rujukan baru dalam hukum pidana di Indonesia. Dalam RKUHP ini (Reza et al., 2023), tindak pidana yang berhubungan dengan teknologi informasi dan siber diatur secara detail dan komprehensif pada Buku Kedua, Bab XV, yakni Pasal 479 sampai dengan Pasal 502. Beberapa poin penting dari penjabaran pasal-pasal tersebut mencakup:

- a. **Enkripsi dan Dekripsi:** Pasal 479 dan Pasal 480 berisi ketentuan mengenai praktik enkripsi dan dekripsi yang melanggar hukum. Ini meliputi penyalahgunaan metode kriptografi dan diatur hukumannya.
- b. **Ancaman Keamanan Siber:** Pasal 484 sampai 486 menekankan pada penanganan ancaman keamanan siber, dimana setiap aksi yang dianggap merusak, mengubah, menghapus, menghilangkan, mentransfer, atau merilis informasi dan/atau data elektronik orang lain tanpa hak akan dihukum.
- c. **Pelanggaran Privasi:** Pasal dalam RKUHP ini, seperti Pasal 491 dan Pasal 492, juga melindungi privasi individu dengan menentukan ancaman pidana bagi mereka yang melakukan intersepsi ilegal komunikasi elektronik dan/atau data elektronik.
- d. **Penipuan Elektronik dan Kejahatan Serupa:** Pasal 497 sampai

Pasal 500 berfokus pada jenis-jenis penipuan dan kekejian lainnya yang dilakukan melalui teknologi informasi.

- e. **Isu Terkait Konten:** Beberapa pasal, seperti Pasal 502, membahas isu-isu terkait konten, seperti penyebaran konten ilegal, pornografi, serta ujaran kebencian dan pencemaran nama baik. Namun, RKUHP ini masih dalam status rancangan dan belum diundangkan, sehingga masih mungkin terjadi perubahan dan penambahan pada Pasal-pasal terkait di atas. Setiap perubahan yang terjadi akan berpengaruh pada bagaimana Indonesia menangani berbagai isu dan tantangan siber di masa depan.

IV. KESIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat disimpulkan bahwa perkembangan regulasi hukum pidana di Indonesia untuk menangkal kejahatan siber terus dilakukan agar sejalan dengan modus operandi kriminal yang makin canggih. UU ITE beserta perubahannya hingga saat ini masih menjadi dasar utama pengaturan tindak pidana di dunia maya. Namun, UU ITE dinilai masih terlalu umum dan multi-tafsir sehingga rawan disalahartikan dalam implementasinya. Oleh karena itu, RKUHP berusaha menyempurnakan rumusan pasal-pasal terkait kejahatan siber agar lebih terukur dan tegas. RKUHP telah merinci dengan lebih komprehensif berbagai jenis cybercrime beserta ancaman pidana yang lebih tinggi untuk memberi efek jera.

Walaupun regulasi telah dilengkapi, tanpa penegakan hukum yang optimal dan konsisten, penanggulangan kejahatan siber tidak akan efektif. Diperlukan upaya serius dari aparat penegak hukum dan pemangku kebijakan terkait untuk mencegah perkembangan kasus yang terus meningkat setiap tahunnya tersebut. Peningkatan kapasitas sumber daya manusia dan infrastruktur hukum juga mutlak diperlukan untuk menjamin proses hukum yang akuntabel dan transparan bagi pelaku kejahatan siber tanpa celah.

DAFTAR PUSTAKA

Interaktif. *Gema Keadilan*, 10(3), 170-182.

- Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, 2(2), 3.
- Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). PENERAPAN HUKUM DALAM MENANGGULANGI KEJAHATAN SIBER PENEGAKAN HUKUM TERHADAP TINDAK PIDANA SIBER. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, 1(6), 8-20.
- Nuralifa, F. (2023). Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial Dihubungkan Dengan Pasal 27 Ayat (3) Juncto Pasal 45 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Kebaruan*, 1(1), 25-32.
- Parulian, H., & Putranto, R. D. (2022). Pidana Ujaran Kebencian Melalui Media Sosial Ditinjau dalam Perspektif Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). *Jurnal Pendidikan dan Konseling (JPDK)*, 4(4), 4909-4919.
- Reza, R. D., Setyorini, S., & Karang, L. (2023). "PENEGAKAN HUKUM PENYALAHGUNAAN MEDIA SOSIAL UNTUK BULLYING DALAM PERSPEKTIF UNDANG-UNDANG INFORMASI TRANSAKSI ELEKTRONIK DAN HUKUM PIDANA ISLAM". *Wasatiyah: Jurnal Hukum*, 4(2), 19-35.
- Supanto, S., Ismunarno, I., Parwitasari, T. A., Budyatmojo, W., Fitriyono, R. A., & Widiyanti, S. (2023). Pencegahan dan Penanggulangan Kejahatan Teknologi Informasi di Wilayah Pdm Kabupaten Klaten melalui Metode Sosialisasi