9

ANALISA YURIDIS PASAL-PASAL KHUSUS TERKAIT KEJAHATAN SIBER DALAM KUHP BARU (UU 1/2023)

Yosua Hia
5222221018@univpancasila.ac.id

Abstrak

Penelitian ini menyelidiki analisis yuridis terhadap pasal-pasal khusus terkait kejahatan siber dalam Kitab Undang-Undang Hukum Pidana (KUHP) baru Indonesia (UU No. 1 Tahun 2023). Dengan menggunakan metode yuridis normatif, penelitian ini menilai efektivitas dan kelengkapan regulasi baru dalam menangani berbagai bentuk kejahatan siber. Hasil penelitian menunjukkan bahwa UU No. 1 Tahun 2023 menyediakan kerangka hukum yang lebih kuat dibandingkan dengan regulasi sebelumnya, dengan merinci elemen-elemen tindak pidana kejahatan siber secara jelas dan menetapkan sanksi yang signifikan untuk mencegah aktivitas tersebut.

Kata Kunci: Analisis Yuridis, Kejahatan Siber, KUHP, UU No. 1 Tahun 2023

Abstract

This research investigates the legal analysis of specific articles related to cybercrime in Indonesia's new Criminal Code (Law No. 1 of 2023). Using a normative juridical method, the study examines the effectiveness and comprehensiveness of the new regulations in addressing various forms of cybercrime. The findings reveal that Law No. 1 of 2023 provides a more robust legal framework compared to previous regulations, detailing clear elements of cybercrime offenses and imposing significant penalties to deter such activities.

Keywords*: Criminal Code, Cybercrime, Law No. 1 of 2023, Legal Analysis*

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan dampak signifikan pada berbagai aspek kehidupan, termasuk dalam bidang hukum[1]. Kemajuan ini tidak hanya membawa manfaat, tetapi juga

[1] Suyanto Sidik. "Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat." Jurnal Ilmiah Widya, Vol. 1, No. 1, 2013, hlm. 3.

tantangan baru, terutama dalam bentuk kejahatan siber. Kejahatan siber atau *cybercrime* mencakup berbagai tindakan ilegal yang dilakukan melalui jaringan komputer dan internet, seperti *hacking*, penyebaran *malware*, pencurian data, dan penipuan *online*[2].

Di Indonesia, peningkatan jumlah kasus kejahatan siber telah mendorong pemerintah untuk mengembangkan kerangka hukum yang lebih kuat dan relevan. UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian diperbarui melalui UU Nomor 19 Tahun 2016, menjadi landasan utama dalam penanganan kejahatan siber di Indonesia. Meskipun demikian, implementasi UU ITE masih menghadapi berbagai tantangan, seperti kurangnya kesadaran hukum di kalangan penegak hukum dan masyarakat, serta keterbatasan infrastruktur dan sumber daya untuk menangani kejahatan siber[3].

Kejahatan siber di Indonesia tidak hanya terbatas pada penipuan *online*, tetapi juga mencakup bentuk-bentuk lain seperti *cyberterrorism* dan *cyberpornography*. Misalnya, kejahatan yang melibatkan kekerasan seksual terhadap anak di dunia maya menunjukkan kekosongan norma dalam UU ITE terkait sanksi yang dikenakan pada pelaku. Hal ini menegaskan perlunya perbaikan hukum yang lebih spesifik untuk mengatasi kejahatan siber yang kompleks dan dinamis[4].

Pentingnya kebijakan hukum yang responsif terhadap perkembangan teknologi dan modus operandi kejahatan siber menuntut adanya revisi dan pembaruan terus-menerus pada regulasi yang ada. Kebijakan ini harus mampu mengimbangi kecepatan evolusi kejahatan siber dan memberikan perlindungan yang efektif bagi masyarakat[5]. Selain itu, kolaborasi internasional menjadi penting mengingat sifat lintas batas dari kejahatan siber yang seringkali melibatkan pelaku dari berbagai negara[6].

---

[2] R Jhon, "Existence of Criminal Law on Dealing Cyber Crime in Indonesia", Vol. 3, 2018, hlm. 25.

[3] Mahrina, Joko Sasmito, Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", Pena Justisia: Media Komunikasi dan Kajian Hukum, Vol. 21, No. 2, December 2022, hlm. 345

[4] Nyoman Juwita Arsawati, I Made Wirya Darma, Putu Eva Ditayani Antari, "A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws", International Journal of Criminology and Sociology, Vol. 10, Februari 2020, hlm. 219

[5] Bambang Tri Bawono et al, "Reformation of Law Enforcement of Cyber Crime in Indonesia", Jurnal Pembaharuan Hukum, Vol. 6, No. 3, 2019, hlm. 332

[6] Broadhurst, R., et al, "Cybercrime in Asia: Trends and Challenges", Development Economics: Regional & Country Studies eJournal, 2012, hlm. 77

Menurut penelitian, pengembangan strategi yang efektif untuk pencegahan dan penanganan kejahatan siber harus melibatkan pendekatan teknologi dan hukum yang komprehensif. Misalnya, pendekatan forensik digital yang kuat sangat diperlukan untuk mengumpulkan dan mengamankan bukti digital yang dapat digunakan dalam proses penegakan hukum[7].

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) baru yang relevan dengan kejahatan siber. Langkah ini diambil untuk memahami sejauh mana regulasi hukum yang ada dapat mengakomodasi dan mengatasi berbagai bentuk kejahatan siber, seperti *hacking*, penyebaran *malware*, pencurian data, penipuan *online*, dan *cyberterrorism*. Selain itu, penelitian ini juga akan menilai efektivitas dan kelengkapan pasal-pasal tersebut dalam menangani kejahatan siber, dengan melihat apakah regulasi yang ada sudah cukup memadai atau masih membutuhkan penyesuaian dan perbaikan. Analisis ini diharapkan dapat memberikan gambaran yang jelas mengenai kesiapan hukum Indonesia dalam menghadapi tantangan kejahatan siber di era digital ini.

Oleh karena itu, jurnal ini akan mengkaji secara mendalam pasal-pasal khusus yang mengatur kejahatan siber dalam Kitab Undang-Undang Hukum Pidana (KUHP) baru di Indonesia, dengan rumusan masalah: "Bagaimana analisa yuridis pasal-pasal khusus terkait kejahatan siber dalam KUHP baru (UU 1/2023) Indonesia?".

II. PEMBAHASAN

Kejahatan digital, atau yang lebih dikenal sebagai kejahatan siber, memiliki definisi resmi dalam berbagai sumber hukum di Indonesia. Berdasarkan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), kejahatan siber dijelaskan sebagai tindakan yang melawan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya[8].

Menurut Pasal 1 ayat 1 UU ITE, yang dimaksud dengan ***"Informasi Elektronik"*** adalah[9]:

---

[7] Anggraeny, Isdian, et al., "The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department." KnE Social Sciences, October 2022, hlm. 349

[8] UU Nomor 11 Tahun 2008.

[9] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

> *"satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronik data interchange (EDI), surat elektronik (electronic mail), telegram, telex, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki makna atau dapat dipahami oleh orang yang mampu memahaminya."*

Kemudian, Pasal 1 ayat 2 UU ITE mendefinisikan ***"Transaksi Elektronik"*** sebagai[10]:

> *"perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya."*

Berdasarkan UU ITE ini, kejahatan siber mencakup segala bentuk aktivitas yang melanggar hukum dengan menggunakan sistem elektronik atau media elektronik lainnya, yang sering kali melibatkan tindakan seperti *hacking*, penyebaran *malware*, penipuan *online*, pencurian data, dan berbagai tindakan ilegal lainnya yang dilakukan melalui internet.

Selain UU ITE, definisi kejahatan siber juga dapat ditemukan dalam berbagai literatur hukum dan kamus hukum. Menurut Kamus Hukum yang diterbitkan oleh *Black's Law Dictionary*, kejahatan siber (*cybercrime*) diartikan sebagai[11]:

> *"Criminal activity or a crime that involves the Internet, a computer system, or computer technology."*

Dalam konteks KUHP baru, kejahatan siber melibatkan berbagai bentuk aktivitas ilegal yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, termasuk komputer, jaringan komputer, dan media elektronik lainnya.

Namun, dalam UU No. 1 Tahun 2023 ini, tidak ada definisi spesifik yang secara eksplisit mencantumkan istilah "kejahatan siber" atau "*cybercrime*." Sebaliknya, undang-undang ini mengatur berbagai tindakan ilegal yang dapat dikategorikan sebagai kejahatan siber, dengan fokus pada aspek-aspek seperti akses ilegal, perusakan data, dan penggunaan teknologi untuk tujuan kriminal.

Berdasarkan penelusuran peneliti terhadap UU Nomor 1 Tahun 2023, tidak ditemukan definisi spesifik untuk istilah "Kejahatan Siber", "Kejahatan Digital", atau "*Cybercrime*". Namun, berbagai bentuk tindak pidana terkait teknologi

[10] Ibid

[11] Black's Law Dictionary, Seventh Edition. United States of America: West Group, 1999.

informasi dan elektronik diatur dalam beberapa pasal di undang-undang tersebut.

Berdasarkan UU Nomor 1 Tahun 2023[12], jenis kejahatan siber atau kejahatan elektronik atau kejahatan berbasis internet (yang sesuai dengan definisi *cybercrime* secara internasional juga berdasarkan UU ITE[13]) dalam KUHP baru dapat diketahui pada **Bagian Kelima "Tindak Pidana terhadap Informatika dan Elektronika"**meliputi:

1. Akses ilegal (Pasal 332);
2. Serangan siber pada system informasi dan infrastruktur negara, pemerintah, dan masyarakat (Pasal 333);
3. Serangan Siber terhadap keuangan, perbankan, dan pemerintah (Pasal 334 dan Pasal 335;

Dengan demikian, berbagai bentuk kejahatan siber yang diatur dalam UU Nomor 1 Tahun 2023 ini sejalan dengan definisi kejahatan siber internasional sebagai aktivitas kriminal yang melibatkan internet, sistem komputer, atau teknologi komputer.

Undang-Undang ini menetapkan sanksi yang berat bagi pelanggaran-pelanggaran tersebut untuk melindungi keamanan dan integritas sistem dan informasi elektronik di Indonesia.

1. Pasal 332 UU No. 1 Tahun 2023 mengenai Akses Ilegal

a. Pasal 332 ayat (1) UU No. 1 Tahun 2023[14]

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau sistem elektronik milik Orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V."

Unsur-unsur Tindak Pidana:

Unsur Subjektif:

- *Kesengajaan*: Tindak pidana ini mensyaratkan adanya unsur kesengajaan, yaitu pelaku dengan sadar dan bermaksud untuk mengakses komputer dan/atau sistem elektronik milik orang lain tanpa izin.

[12] Undang-Undang No. 1 Tahun 2023 tentang KUHP Nasional

[13] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

[14] Pasal 332 ayat (1) UU No. 1 Tahun 2023

Unsur Objektif:

- *Setiap Orang*: Yang dimaksud dengan "setiap orang" di sini adalah subjek hukum yang dapat dikenai sanksi pidana sesuai dengan peraturan perundang-undangan yang berlaku.
- *Tanpa Hak atau Melawan Hukum*: Akses yang dilakukan tanpa hak atau melawan hukum berarti tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik.
- *Mengakses Komputer dan/atau Sistem Elektronik*: Yang dimaksud dengan akses di sini adalah tindakan masuk atau mencoba masuk ke dalam suatu sistem komputer atau jaringan elektronik.
- *Milik Orang Lain*: Komputer atau sistem elektronik yang menjadi objek tindak pidana adalah milik pihak lain, bukan milik pelaku.

Sanksi Pidana:

Sanksi yang diberikan berupa pidana penjara maksimal 6 tahun atau denda kategori V (sebesar Rp 500 juta). Sanksi ini dianggap cukup berat untuk memberikan efek jera kepada pelaku dan menegakkan keadilan bagi korban.

b. Pasal 332 ayat (2) UU No. 1 Tahun 2023[15]

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau system elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/ atau dokumen elektronik, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V."

Unsur-unsur Tindak Pidana:

Unsur Subjektif:

- *Kesengajaan*: Tindak pidana ini mensyaratkan adanya unsur kesengajaan, yaitu pelaku dengan sadar dan bermaksud untuk mengakses komputer dan/atau sistem elektronik milik orang lain tanpa izin dengan tujuan tertentu.

Unsur Objektif:

- *Setiap Orang*: Yang dimaksud dengan "setiap orang" di sini adalah subjek hukum yang dapat dikenai sanksi pidana sesuai dengan peraturan perundang-undangan yang berlaku.

[15] Pasal 332 ayat (2) UU No. 1 Tahun 2023

- *Tanpa Hak atau Melawan Hukum*: Akses yang dilakukan tanpa hak atau melawan hukum berarti tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik.
- *Mengakses Komputer dan/atau Sistem Elektronik*: Yang dimaksud dengan akses di sini adalah tindakan masuk atau mencoba masuk ke dalam suatu sistem komputer atau jaringan elektronik.
- *Dengan Tujuan untuk Memperoleh Informasi Elektronik dan/atau Dokumen Elektronik*: Akses yang dilakukan dengan tujuan untuk mendapatkan informasi elektronik atau dokumen elektronik yang bukan haknya.

Sanksi Pidana:

Sanksi yang diberikan berupa pidana penjara maksimal 7 tahun atau denda kategori V (sebesar Rp 500 juta). Sanksi ini dianggap cukup berat untuk memberikan efek jera kepada pelaku dan menegakkan keadilan bagi korban.

c. Pasal 332 ayat (3) UU No. 1 Tahun 2023[16]

> *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI."*

Unsur-unsur Tindak Pidana:

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk mengakses komputer dan/atau sistem elektronik dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Unsur Objektif:

- *Setiap Orang*: Yang dimaksud dengan "setiap orang" di sini adalah subjek hukum yang dapat dikenai sanksi pidana sesuai dengan peraturan perundang-undangan yang berlaku.
- *Tanpa Hak atau Melawan Hukum*: Akses yang dilakukan tanpa hak atau melawan hukum berarti tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik.

[16] Pasal 332 ayat (3) UU No. 1 Tahun 2023

- *Mengakses Komputer dan/atau Sistem Elektronik*: Yang dimaksud dengan akses di sini adalah tindakan masuk atau mencoba masuk ke dalam suatu sistem komputer atau jaringan elektronik.
- *Dengan Melanggar, Menerobos, Melampaui, atau Menjebol Sistem Pengamanan:* Tindakan akses dilakukan dengan cara yang melibatkan pelanggaran terhadap mekanisme pengamanan yang ada pada komputer atau sistem elektronik tersebut.

Sanksi Pidana:

Sanksi yang diberikan berupa pidana penjara maksimal 7 tahun atau denda kategori VI (sebesar Rp 2 Milyar). Sanksi ini dianggap cukup berat untuk memberikan efek jera kepada pelaku dan menegakkan keadilan bagi korban

2. Pasal 333 UU No. 1 Tahun 2023[17] Mengenai Serangan Siber pada Sistem Informasi dan Infrastruktur Negara, Pemerintah, dan Masyarakat

"*Dipidana dengan pidana penjara paling lama 7 (tqjuh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:*

a. tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apa pun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atauhubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara atau hubungan dengan subjek hukum internasional;

b. tanpa hak melakukan tindakan yang menyebabkan transmisi dari program, informasi, kode atau perintah Komputer atau system elektronik yang dilindungi negara menjadi rusak;

c. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh informasi dari Komputer atau sistem elektronik yang dilindungi oleh negara;

d. tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik milik pemerintah;

e. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh negara, yang

[17] Pasal 333 UU No. 1 Tahun 2023

mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

f. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

g. memengaruhi atau mengakibatkan terganggunya Komputer atau sistem elektronik yang digunakan oleh pemerintah;

h. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos Komputer atau sistem elektronik dengan tujuan menyalahgunakan Komputer atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah; atau

i. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak Komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditqjukan kepada siapa pun."

Unsur-unsur Tindak Pidana:

a. Menggunakan atau Mengakses Komputer Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan atau mengakses komputer atau sistem elektronik tanpa izin dengan tujuan tertentu yang berbahaya.

Unsur Objektif:

- *Setiap Orang*: Merujuk pada subjek hukum yang dapat dikenai sanksi pidana sesuai peraturan perundang-undangan yang berlaku.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.
- *Dengan Maksud*: Tindakan dilakukan dengan tujuan untuk memperoleh, mengubah, merusak, atau menghilangkan informasi.

- *Informasi Pertahanan Nasional atau Hubungan Internasional*: Informasi yang terkait dengan pertahanan negara atau hubungan dengan subjek hukum internasional.
- *Dapat Menyebabkan Gangguan atau Bahaya*: Tindakan tersebut memiliki potensi untuk menyebabkan gangguan atau bahaya terhadap negara atau hubungan internasional.

b. Melakukan Tindakan yang Menyebabkan Kerusakan Transmisi

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk melakukan tindakan yang menyebabkan kerusakan pada transmisi program, informasi, kode, atau perintah dari komputer atau sistem elektronik yang dilindungi negara.

Unsur Objektif:

- *Setiap Orang*: Merujuk pada subjek hukum yang dapat dikenai sanksi pidana sesuai peraturan perundang-undangan yang berlaku.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait penggunaan atau akses terhadap komputer dan/atau sistem elektronik.
- *Melakukan Tindakan yang Menyebabkan Kerusakan*: Mengakibatkan kerusakan pada transmisi dari program, informasi, kode, atau perintah komputer atau sistem elektronik.
- *Sistem Elektronik yang Dilindungi Negara*: Merujuk pada sistem elektronik yang memiliki proteksi khusus oleh negara karena kepentingan keamanan dan integritas informasi.

c. Melampaui Wewenang Menggunakan atau Mengakses Komputer

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk melampaui wewenangnya dalam menggunakan atau mengakses komputer atau sistem elektronik.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak atau Melampaui Wewenang*: Tindakan dilakukan tanpa izin atau melebihi batas wewenang yang dimiliki terkait akses terhadap komputer dan/atau sistem elektronik.

- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.
- *Informasi yang Dilindungi oleh Negara*: Informasi yang memiliki proteksi khusus oleh negara karena kepentingan keamanan.

d. Menggunakan atau Mengakses Komputer Milik Pemerintah

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan atau mengakses komputer atau sistem elektronik milik pemerintah tanpa izin.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik milik pemerintah.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik milik pemerintah.

e. Melampaui Wewenang yang Mengakibatkan Kerusakan

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk melampaui wewenangnya dalam menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan kerusakan.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak atau Melampaui Wewenang*: Tindakan dilakukan tanpa izin atau melebihi batas wewenang yang dimiliki terkait akses terhadap komputer dan/atau sistem elektronik.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.
- *Sistem Elektronik yang Dilindungi oleh Negara*: Merujuk pada sistem elektronik yang memiliki proteksi khusus oleh negara.

- *Mengakibatkan Kerusakan*: Tindakan tersebut mengakibatkan kerusakan pada sistem elektronik tersebut.

f. Melampaui Wewenang yang Mengakibatkan Kerusakan pada Sistem Masyarakat

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk melampaui wewenangnya dalam menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan kerusakan.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak atau Melampaui Wewenang*: Tindakan dilakukan tanpa izin atau melebihi batas wewenang yang dimiliki terkait akses terhadap komputer dan/atau sistem elektronik.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.
- *Sistem Elektronik yang Dilindungi oleh Masyarakat*: Merujuk pada sistem elektronik yang memiliki proteksi khusus oleh masyarakat.
- *Mengakibatkan Kerusakan*: Tindakan tersebut mengakibatkan kerusakan pada sistem elektronik tersebut.

g. Mengganggu Komputer Pemerintah

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk memengaruhi atau mengakibatkan terganggunya komputer atau sistem elektronik yang digunakan oleh pemerintah.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Memengaruhi atau Mengakibatkan Terganggunya*: Tindakan yang memengaruhi atau mengakibatkan terganggunya komputer atau sistem elektronik.
- *Komputer atau Sistem Elektronik yang Digunakan oleh Pemerintah*: Merujuk pada komputer atau sistem elektronik yang digunakan oleh instansi pemerintah.

h. Menyebarkan atau Memperdagangkan Kode Akses

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menyebarkan, memperdagangkan, atau memanfaatkan kode akses atau informasi serupa.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Menyebarkan, Memperdagangkan, atau Memanfaatkan*: Tindakan menyebarkan, memperdagangkan, atau memanfaatkan kode akses atau informasi serupa.
- *Kode Akses atau Informasi Serupa*: Informasi yang dapat digunakan untuk menerobos komputer atau sistem elektronik.
- *Tujuan Menyalahgunakan*: Dengan tujuan menyalahgunakan komputer atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah.

i. Melakukan Perbuatan Merusak dalam Hubungan Internasional

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Melakukan Perbuatan*: Tindakan yang dilakukan dalam rangka hubungan internasional.
- *Maksud Merusak*: Tindakan dilakukan dengan maksud merusak komputer atau sistem elektronik.
- *Komputer atau Sistem Elektronik yang Dilindungi Negara*: Merujuk pada komputer atau sistem elektronik yang dilindungi oleh negara dan berada di wilayah yurisdiksi Indonesia.

Sanksi Pidana:

Pidana Penjara:

Ancaman pidana penjara paling lama 7 tahun. Sanksi ini menunjukkan keseriusan dari tindak pidana ini mengingat dampak yang ditimbulkan bisa sangat besar terhadap keamanan negara dan hubungan internasional.

Pidana Denda:

Ancaman pidana denda paling banyak kategori VI, yaitu denda dengan jumlah antara Rp 2 Miliar. Sanksi denda ini bertujuan untuk memberikan efek jera kepada pelaku serta kompensasi terhadap kerugian yang ditimbulkan dari tindak pidana ini.

Pasal 333 UU No. 1 Tahun 2023 memberikan perlindungan yang komprehensif terhadap akses ilegal yang dapat mengancam sistem informasi dan infrastruktur negara, pemerintah, dan masyarakat. Sanksi yang ditetapkan cukup berat, baik dari sisi pidana penjara maupun denda, untuk memastikan bahwa pelaku mendapat hukuman yang setimpal dan memberikan efek jera.

3. Pasal 334 UU No. 1 Tahun 2023 Mengenai Serangan Siber pada Sistem Keuangan dan Perbankan[18]

"Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:

a. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayar€rn atau yang mengandung data laporan nasabahnya;

b. tanpa hak menggunakan data atau mengakses dengan cara apa pun kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk memperoleh keuntungan;

c. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik bank sentral, Lembaga perbankan atau lembaga keuangan yang dilindungi, dengan maksud menyalahgunakan, atau untuk mendapatkan keuntungan daripadanya; atau

d. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos Komputer atau sistem elektronik dengan maksud menyalahgunakan yang akibatnya dapat memengaruhi system elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri."

[18] Pasal 334 UU No. 1 Tahun 2023

Unsur-unsur Tindak Pidana:

a. Menggunakan atau Mengakses Komputer Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan atau mengakses komputer atau sistem elektronik tanpa izin dengan tujuan memperoleh keuntungan atau informasi keuangan.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana sesuai peraturan perundang-undangan yang berlaku.
- *Tanpa Hak atau Melampaui Wewenang*: Tindakan dilakukan tanpa izin atau melampaui batas wewenang yang dimiliki terkait akses terhadap komputer dan/atau sistem elektronik.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.
- *Informasi Keuangan*: Informasi yang terkait dengan keuangan dari bank sentral, lembaga perbankan, atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran.
- *Maksud Memperoleh Keuntungan*: Tujuan dari tindakan tersebut adalah untuk mendapatkan keuntungan.

b. Menggunakan Data atau Mengakses Kartu Kredit Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan data atau mengakses kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk memperoleh keuntungan.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait penggunaan atau akses terhadap kartu kredit atau kartu pembayaran milik orang lain.
- *Menggunakan Data atau Mengakses*: Melakukan tindakan penggunaan data atau akses ke dalam sistem yang terkait dengan

kartu kredit atau kartu pembayaran.

- Maksud Memperoleh Keuntungan: Tujuan dari tindakan tersebut adalah untuk mendapatkan keuntungan.

c. Mengakses Sistem Elektronik Keuangan yang Dilindungi Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan atau mengakses sistem elektronik yang dilindungi tanpa izin dengan tujuan menyalahgunakan atau mendapatkan keuntungan daripadanya.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak atau Melampaui Wewenang*: Tindakan dilakukan tanpa izin atau melampaui batas wewenang yang dimiliki terkait akses terhadap sistem elektronik yang dilindungi.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam sistem elektronik yang dilindungi.
- *Sistem Elektronik yang Dilindungi*: Merujuk pada sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan yang memiliki proteksi khusus oleh negara.
- Maksud Menyalahgunakan atau Mendapatkan Keuntungan: Tindakan dilakukan dengan tujuan menyalahgunakan sistem elektronik tersebut atau mendapatkan keuntungan daripadanya.

d. Menyebarkan atau Memperdagangkan Kode Akses Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menyebarkan, memperdagangkan, atau memanfaatkan kode akses atau informasi serupa yang dapat digunakan untuk menerobos sistem elektronik dengan tujuan menyalahgunakan.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait penyebaran atau perdagangan kode akses.
- *Menyebarkan, Memperdagangkan, atau Memanfaatkan*: Tindakan

menyebarkan, memperdagangkan, atau memanfaatkan kode akses atau informasi serupa.

- *Kode Akses atau Informasi Serupa*: Informasi yang dapat digunakan untuk menerobos komputer atau sistem elektronik.
- *Maksud Menyalahgunakan*: Tujuan dari tindakan tersebut adalah untuk menyalahgunakan sistem elektronik tersebut.
- *Akibatnya Dapat Mempengaruhi Sistem Elektronik*: Tindakan tersebut memiliki potensi untuk memengaruhi sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

Sanksi Pidana:

Pidana Penjara:

Ancaman pidana penjara paling lama 10 tahun. Sanksi ini menunjukkan keseriusan dari tindak pidana ini mengingat dampak yang ditimbulkan bisa sangat besar terhadap keamanan dan integritas sistem keuangan dan perbankan.

Pidana Denda:

Ancaman pidana denda paling banyak kategori VI, yaitu denda dengan jumlah antara Rp 2 Miliar. Sanksi denda ini bertujuan untuk memberikan efek jera kepada pelaku serta kompensasi terhadap kerugian yang ditimbulkan dari tindak pidana ini.

Pasal 334 UU No. 1 Tahun 2023 memberikan perlindungan yang komprehensif terhadap akses ilegal yang dapat mengancam sistem keuangan dan perbankan. Sanksi yang ditetapkan cukup berat, baik dari sisi pidana penjara maupun denda, untuk memastikan bahwa pelaku mendapat hukuman yang setimpal dan memberikan efek jera.

4. Pasal 335 UU No. 1 Tahun 2023 Mengenai Serangan Siber pada Sistem Pemerintah[19]

"Setiap Orang yang tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apa pun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasial<an atau dilindungi, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun atau pidana denda paling banyak kategori VII."

[19] Pasal 335 UU No. 1 Tahun 2023

Unsur-unsur Tindak Pidana:

a. Menggunakan atau Mengakses Komputer Tanpa Hak

Unsur Subjektif:

- *Kesengajaan*: Pelaku dengan sadar dan bermaksud untuk menggunakan atau mengakses komputer atau sistem elektronik tanpa izin dengan tujuan tertentu yang berbahaya.

Unsur Objektif:

- *Setiap Orang*: Subjek hukum yang dapat dikenai sanksi pidana sesuai peraturan perundang-undangan yang berlaku.
- *Tanpa Hak*: Tindakan dilakukan tanpa izin atau melanggar aturan yang berlaku terkait akses terhadap komputer dan/atau sistem elektronik.
- *Menggunakan atau Mengakses*: Melakukan tindakan penggunaan atau akses ke dalam suatu sistem komputer atau jaringan elektronik.

b. Dengan Maksud Memperoleh, Mengubah, Merusak, atau Menghilangkan Informasi

Unsur Subjektif:

- *Maksud Memperoleh, Mengubah, Merusak, atau Menghilangkan:* Pelaku memiliki tujuan tertentu yaitu untuk memperoleh, mengubah, merusak, atau menghilangkan informasi.

Unsur Objektif:

- *Informasi Milik Pemerintah*: Informasi yang dimiliki oleh pemerintah yang memiliki status khusus.
- *Dirahasiakan atau Dilindungi*: Informasi tersebut harus dirahasiakan atau dilindungi karena statusnya yang penting bagi pemerintah.

Sanksi Pidana:

Pidana Penjara:

Ancaman pidana penjara paling lama 12 tahun. Sanksi ini menunjukkan keseriusan dari tindak pidana ini mengingat dampak yang ditimbulkan bisa sangat besar terhadap keamanan dan integritas informasi pemerintah yang rahasia atau dilindungi.

Pidana Denda:

Ancaman pidana denda paling banyak kategori VII, yaitu denda dengan

jumlah antara Rp 5 Miliar. Sanksi denda ini bertujuan untuk memberikan efek jera kepada pelaku serta kompensasi terhadap kerugian yang ditimbulkan dari tindak pidana ini.

Pasal 335 UU No. 1 Tahun 2023 memberikan perlindungan yang komprehensif terhadap akses ilegal yang dapat mengancam keamanan informasi rahasia atau dilindungi milik pemerintah. Sanksi yang ditetapkan cukup berat, baik dari sisi pidana penjara maupun denda, untuk memastikan bahwa pelaku mendapat hukuman yang setimpal dan memberikan efek jera.

III. KESIMPULAN

Berdasarkan analisis yang dilakukan dalam makalah ini mengenai kejahatan siber dalam konteks Kitab Undang-Undang Hukum Pidana (KUHP) baru yang diatur dalam UU No. 1 Tahun 2023, dengan memperhatikan rumusan masalah "Bagaimana analisa yuridis pasal-pasal khusus terkait kejahatan siber dalam KUHP baru (UU 1/2023) Indonesia?", dapat disimpulkan beberapa poin penting sebagai berikut:

1. Kehadiran Regulasi yang Lebih Spesifik dan Komprehensif:
   UU No. 1 Tahun 2023 memberikan landasan hukum yang lebih spesifik dan komprehensif untuk mengatasi berbagai bentuk kejahatan siber dibandingkan dengan UU ITE yang sebelumnya. Regulasi ini dirancang untuk mengakomodasi kompleksitas dan dinamika kejahatan siber yang terus berkembang.
2. Perincian Unsur-unsur Tindak Pidana Kejahatan Siber:
   Pasal-pasal dalam UU No. 1 Tahun 2023 mengatur berbagai tindakan ilegal yang dapat dikategorikan sebagai kejahatan siber. Setiap pasal menjelaskan unsur-unsur tindak pidana yang harus dipenuhi, seperti unsur kesengajaan, akses ilegal, perusakan data, dan penyebaran informasi rahasia.
3. Sanksi yang Ditetapkan untuk Kejahatan Siber:
   UU No. 1 Tahun 2023 menetapkan sanksi pidana yang cukup berat, termasuk pidana penjara dan denda besar. Sanksi ini bertujuan untuk memberikan efek jera dan menegakkan keadilan bagi korban. Misalnya, Pasal 332 mengatur pidana penjara maksimal 8 tahun untuk akses ilegal dengan pelanggaran sistem pengamanan, sedangkan Pasal 335 menetapkan pidana penjara maksimal 12 tahun untuk penghilangan informasi pemerintah yang rahasia.

4. Perlindungan Terhadap Sistem Keuangan dan Perbankan:
   Pasal 334 memberikan perlindungan khusus terhadap serangan siber pada sistem keuangan dan perbankan. Ancaman pidana penjara maksimal 10 tahun dan denda kategori VI menunjukkan keseriusan dalam melindungi stabilitas ekonomi dan keuangan negara.
5. Penghilangan Informasi Pemerintah yang Dirahasiakan:
   Pasal 335 menekankan pentingnya melindungi informasi pemerintah yang harus dirahasiakan atau dilindungi. Ancaman pidana yang berat menunjukkan betapa seriusnya ancaman terhadap informasi rahasia pemerintah.
6. Kebutuhan akan Pembaruan dan Reformasi Hukum Berkelanjutan:
   Penelitian ini menekankan bahwa regulasi yang ada harus terus diperbarui dan disesuaikan dengan perkembangan teknologi dan modus operandi kejahatan siber. Reformasi hukum yang berkelanjutan sangat penting untuk memastikan regulasi tetap relevan dan efektif dalam memberikan perlindungan hukum yang memadai.

Secara keseluruhan, UU No. 1 Tahun 2023 memberikan kerangka hukum yang lebih kuat dan jelas dalam menangani kejahatan siber di Indonesia. Penegakan hukum yang efektif, didukung oleh regulasi yang komprehensif, akan membantu menciptakan lingkungan digital yang lebih aman dan terlindungi bagi masyarakat. Makalah ini menyoroti bahwa analisis yuridis terhadap pasal-pasal dalam UU No. 1 Tahun 2023 menunjukkan kesiapan hukum Indonesia dalam menghadapi tantangan kejahatan siber di era digital ini.

DAFTAR PUSTAKA

Buku

Black's Law Dictionary, Seventh Edition. United States of America: West Group, 1999.

Jurnal

Arsawati, N., Darma, I., & Antari, P., "A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws", International Journal of Criminology and Sociology, Vol. 10, Februari 2020, 219-223

Isdian Anggraeny et al. "The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department." KnE Social Sciences, October 2022, 349–359

Jhon, R, "Existence of Criminal Law on Dealing Cyber Crime in Indonesia", Vol. 3, 2018, 25-34.

Mahrina, M., Sasmito, J., & Zonyfar, C., "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", Pena Justisia: Media Komunikasi dan Kajian Hukum, Vol. 21, No. 2, December 2022, 345-362

R. Broadhurst et al, "Cybercrime in Asia: Trends and Challenges", Development Economics: Regional & Country Studies eJournal, 2012

Sidik, Suyanto. "Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat." Jurnal Ilmiah Widya, Vol. 1, No. 1, 2013, 1-7

Tri Bawono, Bambang et al, "Reformation of Law Enforcement of Cyber Crime in Indonesia", Jurnal Pembaharuan Hukum, Vol. 6, No. 3, 2019, 332-349

Peraturan Perundang-Undangan

Pasal 29 UU 1/2024

Pasal 332 ayat (1) UU No. 1 Tahun 2023

Pasal 332 ayat (2) UU No. 1 Tahun 2023

Pasal 332 ayat (3) UU No. 1 Tahun 2023

Pasal 333 UU No. 1 Tahun 2023

Pasal 334 UU No. 1 Tahun 2023

Pasal 335 UU No. 1 Tahun 2023

Pasal 45 ayat (8) UU 1/2024

Pasal 45 ayat (9) UU 1/2024

Pasal 482 UU 1/2023

Pasal 79 ayat (1) huruf b UU 1/2023

Undang-Undang No. 1 Tahun 2023 tentang KUHP Nasional

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