

## PERTANGGUNGJAWABAN PIDANA PELAKU KEJAHATAN SIBER DI SEKTOR PERBANKAN DIGITAL BERDASARKAN HUKUM PIDANA DI INDONESIA

Yuarezki Rangga Falahta<sup>1</sup>, Rizky Pratama Karo Karo<sup>2</sup>

Program Studi Strata Satu (S-1) Ilmu Hukum Fakultas Hukum, Universitas Dirgantara Marsekal

Suryadarma<sup>1,2</sup>

Email: [yrfalahta@gmail.com](mailto:yrfalahta@gmail.com)

| Informasi                                                                          | Abstract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volume : 3<br>Nomor : 9<br>Bulan : September<br>Tahun : 2026<br>E-ISSN : 3062-9624 | <p><i>The rapid development of digital technology has brought significant changes to the banking sector in Indonesia. However, digital transformation has also created vulnerabilities to various forms of cybercrime, such as hacking, phishing, skimming, identity theft, and data breaches. This normative legal research examines the regulation and application of criminal liability for cybercrime perpetrators in the digital banking sector based on the Electronic Information and Transactions Law (UU ITE). The study employs statutory, conceptual, and case approaches. The findings indicate that although Indonesia has a comprehensive legal framework, the enforcement of criminal liability faces challenges such as cross-border jurisdictional issues, difficulties in digital evidence, anonymity of perpetrators, and the complexity of corporate liability. The research concludes that optimizing enforcement requires strengthening international cooperation, enhancing digital forensic capabilities, and strict compliance by banking institutions. A balanced approach between repressive and preventive measures is essential to protect customers and maintain the stability of the national financial system.</i></p> <p><b>Keyword:</b> Criminal Liability, Cybercrime, Digital Banking, Electronic Information and Transactions Law, Legal Protection.</p> |

### Abstrak

Perkembangan teknologi digital yang pesat telah membawa perubahan signifikan pada sektor perbankan di Indonesia. Namun, transformasi digital juga menciptakan kerentanan terhadap berbagai bentuk kejahatan siber, seperti peretasan, phishing, skimming, pencurian identitas, dan kebocoran data. Penelitian hukum normatif ini mengkaji pengaturan dan penerapan pertanggungjawaban pidana bagi pelaku kejahatan siber di sektor perbankan digital berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Penelitian menggunakan pendekatan perundang-undangan, konseptual, dan kasus. Temuan menunjukkan bahwa meskipun Indonesia memiliki kerangka hukum yang komprehensif, penegakan pertanggungjawaban pidana menghadapi tantangan seperti masalah yurisdiksi lintas batas, kesulitan bukti digital, anonimitas pelaku, dan kompleksitas pertanggungjawaban korporasi. Penelitian menyimpulkan bahwa optimalisasi penegakan memerlukan penguatan kerja sama internasional, peningkatan kapasitas forensik digital, dan kepatuhan ketat lembaga perbankan. Pendekatan seimbang antara represif dan preventif sangat penting untuk melindungi nasabah dan menjaga stabilitas sistem keuangan nasional.

**Kata Kunci :** Pertanggungjawaban Pidana, Kejahatan Siber, Perbankan Digital, Undang-Undang Informasi dan Transaksi Elektronik, Perlindungan Hukum.

## A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era globalisasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Kemudahan akses internet dan digitalisasi layanan menciptakan ruang baru, yaitu dunia maya (*cyberspace*), yang memungkinkan interaksi sosial, ekonomi, dan budaya tanpa batasan geografis (Lessig, 1999: 4-8). Di Indonesia, penetrasi internet yang terus meningkat menjadikan masyarakat semakin bergantung pada teknologi digital untuk berkomunikasi, bertransaksi, mengakses informasi, dan menjalankan aktivitas sehari-hari.

Namun, di balik manfaat tersebut, perkembangan teknologi juga membuka peluang bagi munculnya bentuk-bentuk kejahatan baru yang memanfaatkan media elektronik, yang dikenal dengan istilah *cybercrime* (Budhijanto, 2025: 2-5). *Cybercrime* atau kejahatan dunia maya merupakan salah satu dampak negatif dari revolusi digital. Berbagai bentuk kejahatan seperti pencurian data pribadi (*phishing*), peretasan sistem (*hacking*), penyebaran virus atau *malware*, penipuan daring (*online fraud*), penyebaran konten ilegal, hingga pembobolan rekening bank dan *cyberterrorism* semakin marak terjadi (Cahyono, Erni, & Hidayat, 2025: 1-23). Kejahatan-kejahatan ini tidak hanya merugikan individu secara finansial dan psikologis, tetapi juga mengancam stabilitas ekonomi nasional, keamanan data pemerintah, serta ketertiban umum (Kainde & Satria, 2025: 563-570).

Sektor perbankan digital menjadi salah satu sasaran utama kejahatan siber mengingat tingginya nilai transaksi dan volume data nasabah yang dikelola secara elektronik. Maraknya kasus pembobolan rekening, *skimming*, peretasan sistem *mobile banking*, serta pencurian data pribadi nasabah melalui rekayasa sosial (*social engineering*) menunjukkan bahwa kejahatan siber di sektor perbankan digital telah mencapai tingkat yang mengkhawatirkan (Lendo, 2025). Menurut laporan Badan Siber dan Sandi Negara (BSSN), terdapat 5,2 miliar anomali lalu lintas internet di Indonesia sepanjang Januari hingga pertengahan November 2025, dengan sektor perbankan menjadi salah satu target utama serangan yang kompleks, tidak hanya menyasar sistem inti tetapi juga nasabah dan sistem pendukung layanan pihak ketiga (BSSN, 2025: 15-18). Sementara itu, Indonesia Anti-Scam Centre (IASC) mencatat total kerugian akibat penipuan digital (*scam*) yang menyasar sektor perbankan mencapai Rp 9,1 triliun sepanjang periode 22 November 2024 hingga 14 Januari 2026, dengan rata-rata 700-800 laporan *scam* per hari (Mediana, 2026). Hal ini menunjukkan bahwa masalah ini menjadi isu hukum yang sangat penting dan mendesak untuk ditangani.

Menghadapi ancaman *cybercrime*, Pemerintah Indonesia telah mengupayakan berbagai instrumen hukum. Payung hukum utama dalam menangani kejahatan siber adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, yaitu Undang-Undang Nomor 19 Tahun 2016 dan lebih lanjut disahkan menjadi Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE. Selain UU ITE, terdapat pula Kitab Undang-Undang Hukum Pidana (KUHP) nasional yang baru, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur aspek perlindungan data di sektor keuangan. Sebagaimana diuraikan dalam buku *Hukum Cyber Crime 4.0*, pendekatan legislasi merupakan upaya antisipatif terhadap implikasi konvergensi teknologi informasi dengan membentuk kerangka pengaturan baru yang responsif terhadap fenomena kejahatan digital (Budhijanto, 2025: 2-5). Peraturan perundang-undangan ini mengatur berbagai perbuatan yang dilarang di ruang digital serta ancaman pidananya, termasuk yang secara spesifik menyasar kejahatan di sektor perbankan digital (Atmasasmita, 2020: 112-115).

Meskipun peraturan perundang-undangan telah ada dan terus disempurnakan, penegakan hukum terhadap tindak pidana *cybercrime* di sektor perbankan digital masih menghadapi berbagai tantangan kompleks. Karakteristik *cybercrime* yang lintas batas negara (*cross-border*), anonimitas pelaku yang tinggi, penggunaan alat bukti digital yang mudah rusak atau dimanipulasi, serta perkembangan modus kejahatan yang sangat cepat seringkali menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku utama, alat pembantu, maupun pihak yang turut serta (penyertaan) (Permana & Dirkareshza, 2025: 245-250). Dalam konteks perbankan digital, pelaku seringkali menggunakan jaringan internasional yang melibatkan aktor di berbagai negara, sehingga menyulitkan proses penuntutan dan penentuan yurisdiksi. Selain itu, terdapat pula perdebatan mengenai apakah pelaku korporasi, termasuk pihak internal perbankan itu sendiri, dapat dimintai pertanggungjawaban pidana atas kejahatan siber yang menguntungkan entitas bisnisnya, serta bagaimana penerapan teori-teori pemidanaan dalam menjatuhkan sanksi yang adil dan efektif (Irawan, 2025).

Dalam praktik peradilan, penanganan perkara kejahatan siber di sektor perbankan digital telah menghasilkan berbagai putusan pengadilan yang mencerminkan upaya penegakan hukum terhadap pelaku. Putusan-putusan ini menunjukkan bahwa aparat penegak hukum telah berupaya menerapkan ketentuan UU ITE dan peraturan terkait untuk menjerat pelaku kejahatan siber. Namun, masih terdapat berbagai kendala dalam penerapan pertanggungjawaban pidana, terutama terkait dengan pembuktian unsur kesalahan,

penentuan subjek hukum, dan penjatuhan sanksi yang memberikan efek jera bagi pelaku sekaligus perlindungan bagi korban. Putusan Pengadilan Negeri Jakarta Selatan Nomor 583/Pid.B/2024/PN JKT.SEL dan berbagai putusan lainnya menunjukkan bahwa meskipun telah terjadi perdamaian antara pelaku dan korban, hakim tetap menjatuhkan pidana penjara, yang mengindikasikan bahwa penerapan pertanggungjawaban pidana dalam kejahatan siber masih menghadapi tantangan serius dalam mencapai keseimbangan antara kepastian hukum, keadilan bagi korban, dan efek jera bagi pelaku (Hakim & Putra, 2025).

Contoh kasus yang menggambarkan kompleksitas ini adalah maraknya kejahatan *skimming* dan pembobolan data perbankan, di mana pelaku menggunakan jaringan internasional untuk mencuri data nasabah. Dalam kasus seperti ini, seringkali yang tertangkap hanya "tukang tarik dana" (yang dapat dikualifikasikan sebagai pembantu), sementara otak pelaku utama berada di luar negeri dan sulit dijangkau yurisdiksi hukum Indonesia. Pertanggungjawaban pidana terhadap masing-masing pihak dalam jaringan kejahatan ini menjadi krusial untuk diuraikan secara yuridis, terutama dalam kaitannya dengan penerapan Pasal-pasal UU ITE dan ketentuan pidana di sektor perbankan (Hakim & Putra, 2025). Oleh karena itu, memahami dan mengkaji secara mendalam bagaimana konsep pertanggungjawaban pidana (*criminal liability*) diterapkan terhadap pelaku *cybercrime* di sektor perbankan digital berdasarkan UU ITE menjadi sangat urgen. Kajian ini tidak hanya menyangkut siapa yang dapat dijerat (subjek hukum), tetapi juga bagaimana unsur kesalahan (*mens rea*), kemampuan bertanggungjawab, dan tidak adanya alasan pemaaf atau pembenar diterapkan dalam konteks kejahatan digital di sektor keuangan yang memiliki kekhususan tersendiri (Moeljatno, 2019: 155-160). Dengan pemahaman yang komprehensif, diharapkan dapat ditemukan solusi yuridis yang tepat untuk mengatasi kendala-kendala yang ada, sehingga penegakan hukum siber di sektor perbankan digital berjalan lebih efektif dan memberikan efek jera, sekaligus melindungi kepentingan nasabah dan stabilitas sistem keuangan nasional (Hamzah, 2017: 89-93).

## B. KAJIAN TEORITIS

### 1. Teori Pertanggungjawaban Pidana

Pertanggungjawaban pidana (*criminal liability*) merupakan konsep sentral dalam hukum pidana yang menentukan apakah seseorang dapat dijatuhi pidana atas perbuatannya. Menurut Moeljatno (2019: 155-160), pertanggungjawaban pidana didasarkan pada tiga unsur utama: (1) adanya kemampuan bertanggungjawab pada diri pelaku; (2) adanya hubungan batin (kesalahan) berupa sengaja (*dolus*) atau kealpaan (*culpa*); dan (3) tidak adanya alasan

penghapusan pidana (alasan pembenar dan alasan pemaaf). Dalam konteks kejahatan siber, ketiga unsur ini harus diterapkan dengan mempertimbangkan karakteristik khusus kejahatan digital, seperti anonimitas pelaku, kompleksitas jaringan, dan sifat lintas batas negara.

## 2. Teori Pidanaan

Teori pidanaan yang relevan dalam konteks kejahatan siber meliputi teori absolut (pembalasan), teori relatif (tujuan), dan teori gabungan. Teori absolut menekankan bahwa pidana dijatuhkan sebagai pembalasan atas perbuatan pidana yang dilakukan. Teori relatif menekankan bahwa pidana memiliki tujuan tertentu, seperti pencegahan (deterrence), rehabilitasi, dan perlindungan masyarakat. Teori gabungan menggabungkan kedua pendekatan tersebut, dengan mempertimbangkan baik unsur pembalasan maupun tujuan pidanaan. Dalam konteks kejahatan siber di sektor perbankan digital, penerapan teori pidanaan harus mempertimbangkan dampak kerugian yang besar bagi korban dan sistem keuangan, serta kebutuhan untuk memberikan efek jera bagi pelaku.

## 3. Konsep Cybercrime

*Cybercrime* atau kejahatan siber merupakan tindak pidana yang dilakukan dengan menggunakan teknologi komputer dan internet sebagai sarana, target, atau tempat terjadinya kejahatan. Budhijanto (2025: 2-5) mengklasifikasikan *cybercrime* ke dalam beberapa kategori, termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data komputer; kejahatan yang berkaitan dengan konten; kejahatan yang berkaitan dengan hak cipta; dan kejahatan yang berkaitan dengan komputer. Dalam konteks perbankan digital, bentuk-bentuk *cybercrime* yang paling relevan meliputi akses ilegal (*illegal access*), intersepsi ilegal (*illegal interception*), gangguan data (*data interference*), gangguan sistem (*system interference*), pemerasan elektronik, dan manipulasi data untuk transfer uang.

## 4. Perlindungan Data Pribadi

Perlindungan data pribadi merupakan aspek penting dalam penanganan kejahatan siber di sektor perbankan digital. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur hak subjek data pribadi, kewajiban pengendali data, dan sanksi bagi pelanggaran perlindungan data. Dalam konteks perbankan digital, bank sebagai pengendali data memiliki kewajiban untuk melindungi data nasabah dari akses ilegal, kebocoran, dan penyalahgunaan. Pelanggaran terhadap ketentuan perlindungan data pribadi dapat dikenai sanksi pidana, baik bagi individu maupun korporasi.

## B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif) yang dilakukan dengan meneliti bahan pustaka atau data sekunder sebagai bahan utama. Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dengan menelaah dan menganalisis peraturan perundang-undangan yang relevan seperti UU ITE, UU PDP, dan KUHP; pendekatan konseptual (*conceptual approach*) dengan mengkaji pandangan dan doktrin para ahli hukum mengenai pertanggungjawaban pidana dan kejahatan siber; serta pendekatan kasus (*case approach*) dengan menganalisis putusan-putusan pengadilan yang berkekuatan hukum tetap dalam perkara *cybercrime* perbankan digital. Sumber bahan hukum yang digunakan meliputi bahan hukum primer (peraturan perundang-undangan), bahan hukum sekunder (buku, jurnal, hasil penelitian), dan bahan hukum tersier (kamus hukum dan ensiklopedia). Teknik pengumpulan data dilakukan melalui studi pustaka, sedangkan analisis data menggunakan metode kualitatif dengan melakukan interpretasi terhadap bahan-bahan hukum yang telah diolah untuk menemukan jawaban atas isu hukum yang diteliti.

## C. HASIL DAN PEMBAHASAN

### 1. Pengaturan Pertanggungjawaban Pidana Pelaku Kejahatan Siber di Sektor Perbankan Digital Berdasarkan UU ITE

#### a. Analisis Unsur Tindak Pidana Siber

Berdasarkan UU ITE, kejahatan siber di sektor perbankan digital dapat dikategorikan ke dalam beberapa bentuk tindak pidana. Untuk dapat dipidana, suatu perbuatan harus memenuhi unsur-unsur tindak pidana yang diatur dalam UU ITE. Berikut adalah matriks analisis unsur tindak pidana siber dan pertanggungjawaban pidana:

| No.  | Bentuk Tindak Pidana                              | Pasal UU ITE | Unsur-Unsur                                                      | Pertanggungjawaban Pidana                                                        | Keterkaitan dengan UU Lain                                          |
|------|---------------------------------------------------|--------------|------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------|
| 100% | Akses Ilegal ( <i>Illegal Access</i> )            | Pasal 30     | - Setiap Orang                                                   | Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600.000.000,00 | KUHP Pasal 362 (pencurian); UU PDP Pasal 67 (perolehan data ilegal) |
|      |                                                   |              | - Dengan sengaja dan tanpa hak atau melawan hukum                |                                                                                  |                                                                     |
|      |                                                   |              | - Mengakses komputer dan/atau sistem elektronik milik orang lain |                                                                                  |                                                                     |
| 200% | Intersepsi Ilegal ( <i>Illegal Interception</i> ) | Pasal 31     | - Setiap Orang                                                   | Pidana penjara paling lama 10 tahun dan/atau denda paling                        | UU PDP Pasal 68 (pengungkapan data ilegal)                          |
|      |                                                   |              | - Dengan sengaja dan tanpa hak                                   |                                                                                  |                                                                     |

|      |                                                |                   |                                                                                                                                                                                                                    |                                                                                     |                                                                                        |
|------|------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|      |                                                |                   | - Melakukan intersepsi atas informasi elektronik yang tidak bersifat publik                                                                                                                                        | banyak<br>Rp800.000.000,00                                                          |                                                                                        |
| 300% | Gangguan Data ( <i>Data Interference</i> )     | Pasal 32          | <ul style="list-style-type: none"> <li>- Setiap Orang</li> <li>- Dengan sengaja dan tanpa hak atau melawan hukum</li> <li>- Mengubah, menambah, mengurangi, merusak, atau menghilangkan data elektronik</li> </ul> | Pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2.000.000.000,00  | KUHP Pasal 363 (pencurian dengan pemberatan); UU PDP Pasal 69 (penggunaan data ilegal) |
| 400% | Gangguan Sistem ( <i>System Interference</i> ) | Pasal 33          | <ul style="list-style-type: none"> <li>- Setiap Orang</li> <li>- Dengan sengaja dan tanpa hak atau melawan hukum</li> <li>- Mengganggu atau merusak sistem elektronik</li> </ul>                                   | Pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp800.000.000,00   | -                                                                                      |
| 500% | Pemerasan atau Pengancaman                     | Pasal 27B dan 27C | <ul style="list-style-type: none"> <li>- Setiap Orang</li> <li>- Dengan sengaja dan tanpa hak</li> <li>- Mendistribusikan informasi elektronik berisi ancaman kekerasan atau menakut-nakuti</li> </ul>             | Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00  | KUHP Pasal 368 (pemerasan)                                                             |
| 600% | Manipulasi Data untuk Transfer Uang            | Pasal 35 jo. 51   | <ul style="list-style-type: none"> <li>- Setiap Orang</li> <li>- Dengan sengaja dan tanpa hak</li> <li>- Memindahkan atau mentransfer uang elektronik</li> </ul>                                                   | Pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp4.000.000.000,00 | UU Perbankan Pasal 49 (kerahasiaan data nasabah)                                       |

## b. Analisis Pertanggungjawaban Pidana Pelaku

Pertanggungjawaban pidana pelaku kejahatan siber di sektor perbankan digital didasarkan pada teori pertanggungjawaban pidana yang mensyaratkan tiga unsur utama: (1) adanya kemampuan bertanggungjawab pada diri pelaku, (2) adanya hubungan batin

(kesalahan) berupa sengaja (*dolus*) atau kealpaan (*culpa*), dan (3) tidak adanya alasan penghapus pidana (alasan pembenar dan alasan pemaaf) (Moeljatno, 2019: 155-160).

### 1) Subjek Hukum

UU ITE dan UU PDP mengakui dua subjek hukum yang dapat dimintai pertanggungjawaban pidana, yaitu individu (orang perseorangan) dan korporasi. Pasal 52 UU ITE secara eksplisit mengatur bahwa jika tindak pidana dilakukan oleh korporasi, maka pidana dapat dijatuhkan terhadap korporasi itu sendiri dan/atau pengurusnya. Pasal 71 UU PDP juga mengatur hal serupa. Dalam konteks perbankan digital, korporasi perbankan dapat dimintai pertanggungjawaban pidana jika terbukti lalai dalam menerapkan sistem keamanan siber sesuai dengan standar yang diwajibkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia.

### 2) Unsur Kesalahan (*Mens Rea*)

Unsur kesalahan dalam kejahatan siber di sektor perbankan digital mencakup kesengajaan (*dolus*) dan kealpaan (*culpa*). Kesengajaan diatur dalam Pasal 45-51 UU ITE yang menggunakan frasa "dengan sengaja dan tanpa hak" atau "dengan sengaja dan melawan hukum". Kealpaan dapat ditemukan dalam kasus kelalaian perbankan dalam melindungi data nasabah, yang diatur dalam UU PDP dan peraturan teknis OJK.

### 3) Kemampuan Bertanggungjawab

Pelaku kejahatan siber di sektor perbankan digital harus memiliki kemampuan bertanggungjawab secara fisik dan psikis. Dalam praktik, seringkali pelaku menggunakan identitas palsu atau menjadi bagian dari jaringan kriminal terorganisir yang melibatkan aktor di berbagai negara, sehingga menyulitkan penentuan kemampuan bertanggungjawab pelaku utama (Irawan, 2025).

### c. Keterkaitan Antar Undang-Undang

Penanganan kejahatan siber di sektor perbankan digital memerlukan pendekatan yang terintegrasi. UU ITE menjadi payung utama yang mengatur berbagai bentuk kejahatan siber, UU PDP mengatur aspek perlindungan data pribadi yang sering menjadi sasaran kejahatan siber, KUHP 2023 mengatur asas-asas umum hukum pidana termasuk penyertaan dan percobaan, UU Perbankan mengatur kewajiban perbankan dalam menjaga kerahasiaan data nasabah, dan peraturan teknis OJK serta Bank Indonesia mengatur standar keamanan siber yang harus dipatuhi oleh lembaga perbankan (Permana & Dirkareshza, 2025: 245-250).

| No. | Aspek | UU<br>ITE | UU<br>PDP | KUHP<br>2023 | UU<br>Perbankan | Peraturan<br>Teknis |
|-----|-------|-----------|-----------|--------------|-----------------|---------------------|
|     |       |           |           |              |                 |                     |

|   |                                |                    |                    |                                      |                 |                      |
|---|--------------------------------|--------------------|--------------------|--------------------------------------|-----------------|----------------------|
| 1 | Definisi<br>Kejahatan<br>Siber | Pasal<br>27-<br>37 | Pasal<br>67-<br>70 | Pasal<br>332-<br>335                 | -               | -                    |
| 2 | Perlindungan<br>Data Pribadi   | Pasal<br>26        | Pasal<br>1-66      | -                                    | Pasal 40,<br>47 | POJK 21/2023         |
| 3 | Sanksi<br>Pidana<br>Individu   | Pasal<br>45-<br>51 | Pasal<br>67-<br>70 | Pasal<br>332-<br>335                 | Pasal 49        | -                    |
| 4 | Sanksi<br>Pidana<br>Korporasi  | Pasal<br>52        | Pasal<br>71        | Pasal<br>56-60<br>jo.<br>198-<br>202 | Pasal 49        | -                    |
| 5 | Yurisdiksi                     | Pasal<br>2         | -                  | -                                    | -               | -                    |
| 6 | Alat Bukti<br>Elektronik       | Pasal<br>5         | -                  | Pasal<br>183-<br>184                 | -               | -                    |
| 7 | Manajemen<br>Risiko Siber      | -                  | -                  | -                                    | Pasal 8         | PBI<br>9/15/PBI/2007 |

## 2. Penerapan Pertanggungjawaban Pidana terhadap Pelaku Kejahatan Siber di Sektor Perbankan Digital Berdasarkan UU ITE

Penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber di sektor perbankan digital dalam praktik peradilan menghadapi berbagai tantangan yang kompleks. Hal ini disebabkan oleh karakteristik kejahatan siber yang berbeda dengan kejahatan konvensional, terutama dalam hal pembuktian, penentuan pelaku, dan penentuan yurisdiksi.

### a. Analisis Putusan Pengadilan

Dalam praktik peradilan, putusan-putusan hakim dalam perkara kejahatan siber di sektor perbankan digital menunjukkan bahwa aparat penegak hukum telah berupaya menerapkan ketentuan UU ITE dan peraturan terkait. Namun, masih terdapat berbagai kendala yang mempengaruhi efektivitas penegakan hukum. Putusan hakim seringkali menjatuhkan hukuman di bawah ancaman maksimal yang diatur dalam UU ITE, yang mengurangi efek jera

bagi pelaku dan belum memberikan perlindungan maksimal bagi nasabah dan stabilitas sistem keuangan nasional (Wardani, Fadjar, & JohnLearn, 2024: 584-600).

Kasus-kasus pembobolan rekening dan pencurian data nasabah yang terjadi di Indonesia menunjukkan bahwa penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber di sektor perbankan digital masih belum optimal. Dalam banyak kasus, pelaku yang tertangkap hanya pelaksana lapangan (*field executor*) atau "tukang tarik dana", sementara pelaku utama yang bertindak sebagai otak kejahatan (*mastermind*) berhasil melarikan diri atau berada di luar negeri sehingga tidak dapat dijangkau oleh proses hukum di Indonesia. Hal ini menyebabkan proses hukum seringkali tidak mencapai keadilan substantif bagi korban, karena pelaku utama yang bertanggung jawab atas kerugian besar yang diderita korban tidak dapat dimintai pertanggungjawaban pidana.

Putusan Pengadilan Negeri Jakarta Selatan Nomor 583/Pid.B/2024/PN JKT.SEL menjadi catatan penting dalam implementasi pertanggungjawaban pidana kejahatan siber di Indonesia. Dalam perkara ini, para terdakwa didakwa melakukan tindak pidana yang tergolong ringan dan selama proses persidangan telah terjadi perdamaian antara pelaku dan korban, dengan kerugian yang tergolong ringan serta perbuatan tersebut merupakan tindak pidana pertama kali yang dilakukan oleh para terdakwa. Namun demikian, amar putusan menyatakan para Terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dan menjatuhkan pidana penjara terhadap para Terdakwa. Kasus ini menunjukkan bahwa meskipun telah terjadi perdamaian antara pelaku dan korban, hakim tetap menjatuhkan pidana penjara, yang mengindikasikan bahwa penerapan pertanggungjawaban pidana belum optimal meskipun regulasi pendukung seperti UU ITE dan UU PDP telah tersedia.

## **b. Keadilan Restoratif bagi Korban**

Selain penegakan hukum yang bersifat represif melalui pemidanaan, perlindungan terhadap korban kejahatan siber di sektor perbankan digital juga dapat dilakukan melalui pendekatan keadilan restoratif (*restorative justice*). Pendekatan ini menekankan pada pemulihan kerugian yang diderita korban, perbaikan hubungan sosial yang terganggu, dan partisipasi aktif korban, pelaku, dan masyarakat dalam proses penyelesaian (Zulfa, 2020: 145-150).

Dalam konteks kejahatan siber di sektor perbankan digital, penerapan keadilan restoratif bagi korban mencakup beberapa aspek:

### **1) Restitusi dan Kompensasi**

UU ITE dan UU PDP mengatur kewajiban pelaku untuk membayar restitusi atau ganti rugi kepada korban atas kerugian yang ditimbulkan. Pasal 52A UU ITE mengatur bahwa pidana tambahan berupa pembayaran ganti rugi dapat dijatuhkan kepada pelaku kejahatan siber. UU PDP juga mengatur hak subjek data pribadi untuk mendapatkan ganti rugi atas kerugian yang diderita akibat pelanggaran perlindungan data pribadi. Dalam konteks perbankan digital, restitusi dapat berupa pengembalian dana nasabah yang hilang akibat pembobolan rekening atau pencurian data.

## **2) Pemenuhan Hak-Hak Korban**

Korban kejahatan siber di sektor perbankan digital berhak untuk mendapatkan informasi tentang perkembangan kasus, akses terhadap dokumen-dokumen yang relevan, dan kesempatan untuk menyampaikan pendapat dan keberatan dalam proses peradilan (Rahayu, 2024: 112-115). Selain itu, korban juga berhak untuk mendapatkan pendampingan hukum dan psikologis untuk membantu pemulihan dari trauma yang diderita.

## **3) Mediasi Penal**

Mediasi penal antara korban dan pelaku dengan pendampingan pihak yang kompeten dapat menjadi alternatif penyelesaian perkara kejahatan siber di sektor perbankan digital. Dalam mediasi ini, korban dan pelaku dapat mencapai kesepakatan mengenai bentuk dan besaran ganti rugi, permintaan maaf, dan langkah-langkah pemulihan lainnya. Mediasi penal dapat dilakukan pada tahap penyidikan, penuntutan, atau persidangan dengan persetujuan kedua belah pihak.

## **4) Program Pemulihan Korban**

Pemerintah dan lembaga perbankan perlu menyediakan program pemulihan bagi korban kejahatan siber, termasuk layanan konseling psikologis, bantuan hukum, dan edukasi tentang keamanan siber untuk mencegah terulangnya kejadian serupa. Program ini penting untuk membantu korban pulih dari kerugian finansial dan psikologis yang diderita akibat kejahatan siber.

## **D. KESIMPULAN**

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa pengaturan pertanggungjawaban pidana pelaku kejahatan siber di sektor perbankan digital diatur secara terintegrasi dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya (UU 1/2024), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Kitab Undang-Undang Hukum Pidana

(KUHP) baru (UU 1/2023), serta Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang didukung oleh peraturan teknis dari Otoritas Jasa Keuangan (POJK 21/2023) dan Bank Indonesia (PBI 9/15/PBI/2007). UU ITE mengatur berbagai bentuk kejahatan siber seperti akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), gangguan data (Pasal 32), gangguan sistem (Pasal 33), pemerasan elektronik (Pasal 27B dan 27C), serta manipulasi data untuk transfer uang (Pasal 35 jo. 51) dengan ancaman pidana penjara hingga 12 tahun, sementara UU PDP mengatur sanksi bagi pelaku kebocoran data pribadi (Pasal 67-70) dengan ancaman pidana penjara hingga 6 tahun, dan ketentuan Pasal 52 UU ITE serta Pasal 71 UU PDP memungkinkan korporasi perbankan dimintai pertanggungjawaban pidana jika terbukti lalai menerapkan sistem keamanan siber sesuai standar yang diwajibkan. Namun demikian, penerapan pertanggungjawaban pidana dalam praktik peradilan masih menghadapi berbagai tantangan, antara lain kesulitan identifikasi pelaku utama karena anonimitas dan jaringan lintas negara, kesulitan pengumpulan dan pemeliharaan alat bukti digital yang rentan terhadap manipulasi, penentuan yurisdiksi dalam kejahatan siber lintas batas negara (Pasal 2 UU ITE), serta kompleksitas penerapan unsur kesalahan (*mens rea*) dan kemampuan bertanggungjawab, yang mengakibatkan putusan hakim seringkali berada di bawah ancaman maksimal dan belum memberikan efek jera optimal. Oleh karena itu, diperlukan penguatan kerjasama internasional, peningkatan kapasitas forensik digital aparat penegak hukum, penyusunan pedoman khusus penanganan bukti digital, serta harmonisasi antar regulasi untuk menciptakan kepastian hukum dan meningkatkan efektivitas penegakan hukum kejahatan siber di sektor perbankan digital.

## 2. Saran

Berdasarkan kesimpulan di atas, penelitian ini memberikan saran kepada aparat penegak hukum (kepolisian, kejaksaan, dan hakim) agar meningkatkan kapasitas dan kompetensi teknis di bidang forensik digital melalui pelatihan berkelanjutan, termasuk pemahaman tentang modus operandi kejahatan siber yang terus berkembang seperti pemanfaatan kecerdasan buatan (AI) dan teknologi *blockchain*, serta membentuk unit khusus *cybercrime* yang dilengkapi peralatan forensik digital memadai dan kemampuan penyidikan lintas negara. Hakim diharapkan lebih konsisten dalam menjatuhkan putusan yang mencerminkan rasa keadilan bagi korban dan memberikan efek jera bagi pelaku dengan mempertimbangkan pidana tambahan berupa restitusi sebagaimana diatur dalam Pasal 52A UU ITE dan UU PDP. Kepada pembuat kebijakan dan legislator, disarankan untuk melakukan harmonisasi UU ITE, UU PDP, KUHP baru (UU 1/2023), dan UU Perbankan (UU 10/1998) guna menghindari

tumpang tindih regulasi, menyusun pedoman pembuktian khusus perkara *cybercrime* yang mengakomodasi keunikan alat bukti digital (Pasal 5 UU ITE), serta menguatkan mekanisme kerjasama internasional termasuk perjanjian ekstradisi dan bantuan hukum timbal balik di sektor keuangan. Penguatan kewajiban kepatuhan (*compliance*) bagi lembaga perbankan dalam menerapkan manajemen risiko siber sesuai POJK 21/2023 dan PBI 9/15/PBI/2007 perlu menjadi prioritas dengan sanksi tegas bagi bank yang lalai melindungi data nasabah, serta pemerintah perlu mendorong sosialisasi dan edukasi keamanan siber kepada masyarakat agar lebih waspada terhadap kejahatan siber di sektor perbankan digital.

## **E. DAFTAR PUSTAKA**

### **A. Buku**

- Atmasasmita, R. (2020). Hukum pidana transnasional. Refika Aditama.
- Budhijanto, D. (2025). Hukum cyber crime 4.0: Kejahatan digital dan artificial intelligence (AI). Refika Aditama.
- Hamzah, A. (2017). Asas-asas hukum pidana. Rineka Cipta.
- Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.
- Moeljatno. (2019). Asas-asas hukum pidana. Rineka Cipta.
- Zulfa, E. A. (2020). Keadilan restoratif: Penerapannya dalam tindak pidana penganiayaan. Rajawali Pers.

### **B. Jurnal Ilmiah**

- Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rekonstruksi hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia. Dame Journal of Law, 1(1), 1-23.
- Hakim, M. R., & Putra, M. R. S. (2025). Analysis of digital bank customer protection against loss of funds in accounts reviewed according to Indonesian positive law. Jurnal USM Law Review, 8(2).
- Irawan, D. (2025). Tinjauan yuridis terhadap tindak pidana siber. Jurnal Litbang Polri. Pusat Penelitian dan Pengembangan Polri.
- Kainde, Q. C., & Satria, I. (2025). Telaah filsafat hukum dalam penanggulangan tindak pidana cybercrime di Indonesia. Nomos: Jurnal Penelitian Ilmu Hukum, 5(3), 563-570.
- Lendo, Y. T. (2025). Kajian yuridis terhadap kejahatan pembobolan rekening dalam kasus phishing di sektor perbankan. Lex Privatum. Fakultas Hukum Universitas Sam Ratulangi.
- Permana, F. R., & Dirkareshza, R. (2025). Banking legal liability of cybercrime for the loss of

customer funds in Indonesian digital banks. *Al-Risalah: Jurnal Ilmu Hukum*, 21(2), 245-250.

Rahayu, S. (2024). Kejahatan siber dan perlindungan hukum bagi konsumen perbankan digital. *Jurnal Hukum dan Perbankan Nasional*, 8(2), 112-115.

Wardani, F. D. E. K. E., Fadjar, R. F., & JohnLearn, M. V. (2024). Juridical review of cyber security mobile banking digitalization process for legal protection of customers. *YURISDIKSI: Jurnal Wacana Hukum dan Sains*, 19(4), 584-600.

### **C. Peraturan Perundang-undangan**

Indonesia. (1998). Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Nomor 3790.

Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843.

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 216, Tambahan Lembaran Negara Nomor 6832.

Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Nomor 6842.

Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6932.

Otoritas Jasa Keuangan. (2023). Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum.

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Pemanfaatan Teknologi Informasi oleh Bank.

### **D. Laporan dan Dokumen Resmi**

Badan Siber dan Sandi Negara (BSSN). (2025). Laporan tahunan ancaman siber di Indonesia.

E. Sumber Daring (Berita/Artikel Online)

Mediana, C. (2026, April 16). Ancaman siber dan 'scam' kian ganas. *Kompas.id*.  
<https://www.kompas.id>