BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Fenomena ini kian menjadi sorotan luas seiring dengan akselerasi dunia digital yang secara radikal merombak tatanan hidup masyarakat, terutama dalam urusan komunikasi serta transaksi bisnis. Meski kehadiran teknologi digital sangat mempermudah rutinitas, kemajuan ini ibarat pisau bermata dua yang memberi celah bagi pihak tak bertanggung jawab untuk melakukan eksploitasi yang merugikan. Di antara berbagai bentuk kriminalitas yang paling marak di masa sekarang adalah aksi kriminal di ruang digital atau yang lebih dikenal sebagai kejahatan siber. Praktik ilegal ini memanfaatkan sistem elektronik maupun jaringan komputer, yang kini skalanya terus meluas dengan teknik yang makin canggih. Hal ini memicu kekhawatiran besar di masyarakat, terutama terkait tingginya risiko pencurian serta kebocoran data sensitif saat bertransaksi secara daring, karena tidak hanya mengancam privasi tapi juga berpotensi menimbulkan kerugian materil yang masif. Mengklaim bahwa kolaborasi lintas sektor antara pemerintah, bisnis, dan masyarakat sipil merupakan komponen penting dalam membangun lingkungan keamanan siber yang tangguh. Tanpa kerja sama dan standar nasional yang konsisten, mereka berpendapat bahwa sistem keamanan data akan selalu berada di balik strategi serangan yang terus berkembang. Inisiatif-inisiatif ini juga harus memiliki komponen hukum dan pendidikan, seperti penguatan hukum dan peningkatan pengetahuan publik tentang perlunya menjaga keamanan data pribadi, selain komponen teknologi. Kementerian Komunikasi dan Informatika dan Badan Siber dan Sandi Negara (BSSN) bersama-sama menyatakan bahwa peretasan tersebut berhasil sebagian karena arsitektur keamanan nasional yang lemah dan kurangnya kolaborasi kelembagaan. Perlunya akuntabilitas dan transparansi menjadi jelas ketika desain dan pengelolaan PDN dilakukan secara tertutup tanpa pengawasan bersama. Penggunaan kata sandi sederhana seperti Admin 1234 dan penonaktifan fitur keamanan seperti Windows Defender menunjukkan kurangnya kesiapan dan profesionalisme dalam menangani risiko siber. Masalah ini menyoroti buruknya tata kelola keamanan siber dan budaya Indonesia di samping sifat teknisnya.[1] Salah satu negara yang rentan terhadap serangan siber adalah Indonesia. Hal ini terlihat jelas dari insiden besar pada Juni 2024 ketika terjadi kebocoran data berskala nasional melalui Pusat Data Nasional (PDN) yang dikelola Kementerian Komunikasi dan Informatika (Kemenkominfo). Dengan menggunakan teknik Ransomware, sekelompok pelaku kejahatan siber memblokir akses ke data-data sensitif termasuk kartu tanda penduduk (KTP), Nomor Induk Kependudukan (NIK), nomor telepon, serta informasi identitas pribadi lainnya. Serangan ini memengaruhi sejumlah besar lembaga pemerintah lebih dari 210 serta layanan publik yang krusial termasuk imigrasi. Windows Defender dan sistem keamanan lainnya juga rusak akibat serangan tersebut. Insiden ini menyoroti kelemahan dalam manajemen keamanan sistem digital negara ini, terutama dalam hal kelalaian administratif, sistem pencadangan yang lemah, dan kata sandi yang lemah.[2]

Insiden kejahatan nasional ini menunjukkan kekurangan mendasar dalam tata kelola keamanan siber nasional dalam hal infrastruktur, personel, dan kolaborasi kelembagaan. Risiko yang muncul semakin meningkat dengan aturan yang buruk dan kurangnya tindakan hukum terhadap pelaku kejahatan siber. Maka dari itu, mengapa urgensi penelitian ini terletak pada upaya untuk membongkar mekanisme. pertanggungjawaban pidana dapat ditetapkan kepada pelaku kejahatan siber dalam konteks kebocoran data elektronik, sebagaimana yang terjadi dalam kasus Pusat Data Nasional Kominfo tahun 2024. Penelitian ini dimaksudkan untuk memberikan saran yang mendalam untuk meningkatkan keamanan hak privasi warga negara di era digital serta untuk memperkuat sistem hukum pidana Indonesia.[3]

Dampak ekonominya juga nyata: kepercayaan publik terhadap organisasi pemerintah telah anjlok seiring dengan biaya pemulihan hukum dan sistem. Kerugian finansial dan reputasi yang diakibatkan oleh kebocoran PDN secara langsung memengaruhi kepercayaan, klaim *D'Trust*, yang merupakan dasar legitimasi hukum dan sosial pemerintahan. Hal ini

---

[1] Imanuel Toding Bua dan Nur Isdah Idris," Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024," *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan 2*, no. 2, Mei 2025, hal 100-114.

[2] RA Dyah Wahyu Sukman," Kebocoran Data Nasional: Sebanyak 210 Intansi Kena Bobol," *BINUS University*, 12 November 2024,(https://sis.binus.ac.id/2024/11/12/kebocoran-data-nasional-sebanyak-210-instansi-kena-bobol/, diakses pada 13 Juni 2025).

[3]Grace Mayda dan Rena Elvaretta, "Pembobolan Pusat Data Nasional: Pembelajaran Pemerintah dalam Penguatan Keamanan Perlindungan Data Nasional," Lembaga Kajian dan Konsultasi Hukum Fakultas Hukum Universitas Indonesia (LK2 FHUI), November 2024.

memvalidasi bahwa pelanggaran data adalah krisis ekonomi dan politik, bukan hanya krisis teknis.[4] Dalam konteks hukum, Indonesia telah memiliki UU ITE, PP 82/2012 dan UU No. 27/2022 tentang Perlindungan Data Pribadi. Namun, kelemahan melalui penegakan dan regulasi yang belum komprehensif contohnya sanksi pidana yang samar dalam UU ITE menimbulkan risiko bahwa pelaku kejahatan siber tidak sepenuhnya dipertanggungjawabkan secara hukum. Pemerintah pun dinilai belum menindak tegas instansi yang lalai, padahal ini adalah langkah penting untuk membangun rasa aman publik.[5]

Penelitian ini difokuskan pada kasus kebocoran Pusat Data Nasional (PDN) 2024. Berbeda dengan insiden-insiden sebelumnya, kasus ini langsung memengaruhi infrastruktur negara dan mengganggu lebih dari 210 lembaga pemerintah dan layanan publik penting termasuk imigrasi, keuangan, dan kependudukan. Kasus ini juga unik karena para penyerang berhasil masuk ke sistem utama negara dengan memanfaatkan kelemahan teknis dan administratif yang seharusnya dapat dihindari. Hal ini menghadirkan PDN 2024 sebagai contoh nyata yang mencerminkan kondisi keamanan siber nasional yang sebenarnya, yang belum banyak dibahas dalam penelitian hukum pidana yang ekstensif. Penulis berpendapat bahwa kajian tentang pertanggungjawaban pidana pelaku kejahatan siber, khususnya dalam konteks kebocoran data dan pelanggaran data, belum banyak dikaji khususnya dengan pendekatan hukum normatif dalam konteks kasus PDN. Judul ini dipilih karena alasan tersebut.[6]

Langkah ini diambil dengan tujuan menyumbangkan gagasan baru dalam mendefinisikan bentuk pertanggungjawaban hukum pidana bagi pelaku kejahatan siber yang bertanggung jawab atas kebocoran data serta dalam mendorong perubahan peraturan perundang-undangan dan pelaksanaannya di Indonesia. Mengingat kasus ini melibatkan sistem milik negara dan berdampak pada banyak sektor pelayanan publik di seluruh Indonesia, maka lokasi penelitian bersifat nasional. Dengan menggunakan pendekatan normatif dan studi pustaka, penulis berpendapat bahwa cakupan kasus ini sangat sesuai untuk penelitian hukum.[7]

1.2 RUMUSAN MASALAH

Penyusunan rumusan masalah ditujukan untuk mengerucutkan ruang lingkup penelitian. Berdasarkan hal tersebut, berikut adalah rincian permasalahan yang akan dikaji dalam studi ini adalah:

1. Bagaimana bentuk pola kejahatan siber yang terjadi dalam kasus kebocoran Pusat Data Nasional tahun 2024?
2. Apa jenis pertanggungjawaban pidana yang dapat dikenakan terhadap pelaku kejahatan siber terkait data elektronik, berdasarkan studi kasus kebocoran Pusat Data Nasional Kominfo tahun 2024?
3. Bagaimana efektivitas penerapan sanksi pidana serta kelemahan sistem pengawasan pemerintah terhadap sistem digital nasional berdasarkan peraturan perundang-undangan di Indonesia?

1.3 TUJUAN PENELITIAN

Eksistensi tujuan dan manfaat dalam penelitian dimaksudkan untuk memetakan fokus kajian menunjukkan arah serta kontribusi dari penelitian ini.

1. Mengetahui pola kejahatan siber yang terjadi dalam kasus kebocoran Pusat Data Nasional tahun 2024
2. Mengetahui jenis pertanggungjawaban pidana yang dapat dikenakan terhadap pelaku kejahatan siber terkait data elektronik, berdasarkan studi kasus kebocoran Pusat Data Nasional Kominfo tahun 2024
3. Mengetahui efektivitas penerapan sanksi pidana serta mengidentifikasi kelemahan sistem pengawasan pemerintah terhadap keamanan sistem digital nasional menurut peraturan perundang-undangan di Indonesia.

1.4 MANFAAT PENELITIAN

---

[4] DTrust Team," Kebocoran Data PDNS: Apa yang Terjadi dan Pembelajaran yang Bisa Kita Petik," *DTrust Resources*, dipublikasikan 3 bulan yang lalu (sekitar Maret 2025), (https://resources.dtrust.co.id/blog/kebocoran-data-pdns-apa-yang-terjadi-dan-pelajaran-yang-bisa-kita-petik/, diakses pada 13 Juni 2025).

[5] Naylawati Bahtiar, "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah," *Development Policy and Management Review* 2, no. 1 (Juni 2022): 85–100.

[6] Muhammad Asthi Seta Ari Yuwana, Andhika Pratama Adhi Surya, Abdul Hakim Al Baihaqy, dan M. Asif Nur Fauzi," Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM," *Jurnal Hukum dan Hukum Wicarana 4*, no. 1 (Maret 2025): 31-37.

[7] Bua dan Idris, *Analisis Kebijakan Keamana Siber*, 112-113.

1. Manfaat Teoritis
   Melalui rangkaian penelitian ini, didapatkan hasil kontribusi konseptual guna memperkaya khazanah literatur hukum pidana siber melalui analisis sistematis terhadap pola kejahatan siber dan mekanisme pertanggungjawaban pidana, khususnya dalam konteks kasus kebocoran Pusat Data Nasional tahun 2024, sehingga dapat menjadi rujukan teoretis bagi pengembangan teori dan pemahaman mendalam mengenai dinamika, tantangan, serta kompleksitas penegakan hukum terhadap pelaku kejahatan siber di Indonesia berbasis evaluasi atas regulasi dan efektivitas sanksi pidana yang selama ini berlaku.
2. Manfaat Praktis
   Temuan studi ini ditujukan untuk menjadi bahan pertimbangan strategis dalam pemangku kepentingan, khususnya aparat penegak hukum, legislator, dan pengelola sistem digital pemerintah, dalam perumusan kebijakan dan peningkatan mekanisme penegakan hukum guna memperkuat sistem pengawasan, pengelolaan, serta perlindungan data nasional, sekaligus menjadi
   acuan dalam menyusun langkah-langkah preventif dan represif yang lebih adaptif terhadap ancaman kejahatan siber, terutama terkait kebocoran data dan efektivitas penerapan sanksi pidana terhadap pelaku kejahatan siber pada ranah transaksi elektronik sesuai perkembangan regulasi dan teknologi yang berlaku.

1.5 ORIGINALITAS PENELITIAN

Originalitas penelitian ini terletak pada pemetaan terhadap studi-studi terdahulu yang berkaitan. guna untuk membedakan arah riset saat ini dengan yang sudah ada tetapi juga untuk memanfaatkan temuan lama tersebut sebagai pijakan dalam melahirkan perspektif baru yang belum banyak dikaji oleh peneliti lain.

Setelah meninjau beragam referensi, ditemukan sejumlah studi terdahulu yang memiliki relevansi kuat dengan arah penelitian yang sedang dilakukan saat ini. Pertama, penelitian oleh **Eka Hero Ramadhani, dkk.** yang berjudul *"Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional"* (JIMIK, Vol. 6 No. 1, 2025), menjelaskan bahwa kerentanan pada PDN disebabkan oleh lemahnya manajemen keamanan dari sisi SDM, proses, dan teknologi berdasarkan pendekatan *People, Process, Technology (PPT)*. Fokus penelitian tersebut adalah pada strategi teknis dan manajerial dalam memperkuat sistem terhadap serangan siber, namun tidak membahas pertanggungjawaban hukum secara pidana terhadap pelaku kejahatan siber. Berbeda halnya dengan penelitian ini, yang secara khusus mengkaji aspek pertanggungjawaban pidana pelaku kejahatan siber dalam transaksi elektronik berdasarkan hukum positif di Indonesia.[8]

Kedua, penelitian oleh **Dhina Khoerunisa** berjudul *"Analisis Framing Pemberitaan Peretasan Pusat Data Nasional di Media Online"* (2024), lebih menyoroti bagaimana media seperti DetikNews, CNN Indonesia, dan Tempo membingkai isu kebocoran PDN 2024. Dengan menggunakan pendekatan analisis framing model Entman, penelitian tersebut berfokus pada sudut pandang media dan dampaknya terhadap persepsi publik. Namun, penelitian tersebut tidak mengulas aspek hukum, terutama mengenai pertanggungjawaban pidana pelaku peretasan, sebagaimana yang menjadi fokus utama dalam penelitian ini.[9]

Ketiga, penelitian oleh **Fransiscus Xaverius Watkat, dkk.** dalam artikel *"Pertanggungjawaban Pidana Pengendali Data Pribadi terhadap Kebocoran Data Warga Negara Indonesia"* (Jurnal Hukum Ius Publicum, 2024), menelaah tanggung jawab pidana dari sisi pengendali data pribadi berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Penelitian ini lebih memfokuskan pada kelalaian pihak pengelola data dan lemahnya sanksi pidana dalam UU PDP, bukan pada pelaku kejahatan digital eksternal. Oleh karena itu, penelitian ini mengambil arah berbeda, yakni menganalisis secara yuridis pertanggungjawaban pidana terhadap pelaku serangan siber eksternal terkait data elektronik, sebagaimana yang terjadi dalam kasus kebocoran PDN tahun 2024.[10]Dengan demikian, meskipun telah terdapat berbagai penelitian mengenai kejahatan siber dan perlindungan data, belum ada yang secara spesifik membahas kasus kebocoran PDN 2024 dari perspektif hukum pidana dan pertanggungjawaban pelaku berdasarkan regulasi yang berlaku di Indonesia. Penelitian ini diharapkan dapat memberikan

---

[8] Eka Hero Ramadhani, I Ketut Agung Enriko, dan Erika Lety Istikhomah Puspita Sari, "Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional", *Jurnal Indonesia: Manajemen Informatika dan Komunikasi (JIMIK)*, Vol. 6 No. 1 (2025), hlm. 570–575.

[9] Dhina Khoerunisa, "Analisis Framing Model Robert N. Entman pada Pemberitaan Kebocoran Pusat Data Nasional (PDN) di Media Online", *Jurnal IKRA-ITH Humaniora*, Vol. 8 No. 3 (2024), hlm. 153–157.

[10] Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun, Muhammad Hafiz Ingsaputro, dan Arie Tri Hartantyo, "Pertanggungjawaban Pidana Pengendali Data Pribadi terhadap Kebocoran Data Warga Negara Indonesia", *Jurnal Hukum Ius Publicum*, Vol. 5 No. 2 (2024), hlm. 178–185.

kontribusi baik secara akademik maupun praktis dalam pengembangan hukum pidana siber di Indonesia, khususnya dalam menghadapi tantangan kebocoran data dan perlindungan infrastruktur digital nasional.

Keempat, penelitian oleh **Imanuel Toding Bua dan Nur Isdah Idris** yang berjudul *"Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024"* (Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, Vol. 2 No. 2, Mei 2025, hlm. 100–114), secara khusus mengkaji bagaimana kebijakan keamanan siber nasional diuji dalam menghadapi insiden kebocoran PDN. Penelitian ini menganalisis regulasi yang berlaku, efektivitas koordinasi antar lembaga pemerintah, serta respon kelembagaan terhadap serangan siber yang berdampak luas terhadap layanan publik. Penelitian ini menggunakan pendekatan normatif dan kebijakan publik untuk mengevaluasi sejauh mana kesiapsiagaan sistem keamanan nasional mampu mengantisipasi dan menangani ancaman siber berskala besar. Fokus utama penelitian tersebut berada pada ranah perumusan dan pelaksanaan kebijakan, termasuk bagaimana lemahnya pengawasan, kurangnya integrasi antar instansi, serta ketidaksiapan teknis menjadi faktor utama yang memperburuk dampak dari serangan PDN 2024. Meskipun membahas objek yang sama, yaitu kebocoran data nasional pada Pusat Data Nasional Kominfo, penelitian ini tidak mengulas secara eksplisit tanggung jawab pidana dari pelaku kejahatan siber yang melakukan peretasan. Oleh karena itu, penelitian ini memiliki orientasi yang berbeda dengan penelitian ini, yang secara spesifik menganalisis bentuk pertanggungjawaban pidana terhadap pelaku serangan siber eksternal berdasarkan kerangka hukum pidana yang berlaku di Indonesia. Penelitian oleh Bua dan Idris tetap relevan untuk dijadikan pembanding, karena sama-sama menyoroti kelemahan sistem keamanan siber nasional, namun melalui sudut pandang kebijakan publik dan bukan aspek yuridis pidana[11].

1.6 KERANGKA TEORI DAN KONSEPSI

Bagian ini merangkum teori serta konsep utama yang menjadi pijakan analisis dalam riset ini. Kerangka berpikir tersebut akan membantu memahami fenomena kejahatan siber, khususnya kaitannya dengan kebocoran data dan pertanggungjawaban pidana**.**

1. Kerangka Teori

   Untuk membedah permasalahan yang ada, penelitian ini menerapkan **teori kontrol sosial**. Teori ini menjelaskan bahwa perilaku menyimpang atau tindak pidana dapat terjadi apabila seseorang tidak memiliki keterikatan yang kuat terhadap nilai-nilai sosial, norma hukum, dan lingkungan sekitarnya. Individu cenderung akan menjauh dari tindakan kriminal apabila memiliki hubungan yang erat dengan masyarakat, aktif dalam kegiatan positif, dan meyakini pentingnya mematuhi hukum.

   Terdapat empat komponen utama dalam teori kontrol sosial, yaitu

   a. **Keterikatan (attachment)** – hubungan emosional dengan keluarga, teman, atau institusi sosial yang menumbuhkan rasa peduli terhadap norma sosial.
   b. **Komitmen (commitment)** – keterlibatan dalam aktivitas yang bernilai dan legal seperti pendidikan atau pekerjaan, yang membuat seseorang enggan mengambil risiko melakukan kejahatan.
   c. **Keterlibatan (involvement)** – keikutsertaan dalam kegiatan positif yang mengurangi waktu dan peluang untuk melanggar hukum.
   d. **Kepercayaan (belief)** – keyakinan bahwa hukum dan norma sosial harus dihormati dan ditaati.

Ketika keempat elemen tersebut melemah, maka potensi seseorang untuk melakukan pelanggaran hukum akan semakin besar. Dalam konteks kejahatan siber pada kasus kebocoran Pusat Data Nasional (PDN) tahun 2024, pelaku kejahatan dapat dipahami sebagai individu yang mengalami kegagalan kontrol sosial, seperti lemahnya rasa tanggung jawab, kurangnya kepercayaan terhadap norma hukum, dan tidak adanya keterlibatan dalam kegiatan sosial yang membangun. Oleh karena itu, teori kontrol sosial relevan digunakan sebagai landasan untuk menganalisis faktor penyebab terjadinya tindak pidana siber dan pentingnya penguatan nilai sosial dalam pencegahan kejahatan digital. teori kontrol sosial memberikan kerangka berpikir bahwa perilaku menyimpang bukan semata-mata disebabkan oleh faktor internal pelaku seperti motif atau niat jahat, melainkan juga dipengaruhi oleh lemahnya struktur sosial di sekitarnya. Dalam dunia digital, keterhubungan sosial sering kali digantikan oleh interaksi maya

[11] Imanuel Toding Bua dan Nur Isdah Idris," Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024," *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan 2*, no. 2, Mei 2025, hal 100-114.

yang cenderung anonim dan tidak berbasis nilai kolektif yang kuat. Hal ini menyebabkan individu lebih mudah melakukan pelanggaran hukum tanpa adanya rasa bersalah atau tanggung jawab sosial.

Kejahatan siber seperti pembobolan sistem elektronik PDN kondisi ini bukan mencerminkan ketentuan hukum positif, melainkan juga menunjukkan kegagalan institusi sosial dalam menanamkan nilai, norma, dan kontrol terhadap perilaku masyarakat di ranah digital. Ketidakhadiran pengawasan sosial yang efektif di dunia maya menjadi tantangan serius dalam penegakan hukum. Pelaku dapat merasa tidak diawasi, tidak dikenali, dan bebas dari ikatan sosial yang biasanya menjadi pengendali perilaku dalam kehidupan nyata. Dengan menggunakan teori kontrol sosial, penelitian ini menekankan pentingnya pendekatan preventif berbasis nilai dan pendidikan sosial yang kuat. Penguatan kontrol sosial baik formal maupun informal dapat menjadi strategi jangka panjang untuk mengurangi potensi terjadinya tindak pidana siber. Ini termasuk peningkatan literasi digital, penguatan etika penggunaan teknologi, keterlibatan aktif keluarga dan institusi pendidikan dalam membentuk karakter pengguna internet, serta penanaman rasa tanggung jawab dalam setiap aktivitas digital. Oleh karena itu, teori kontrol sosial tidak hanya relevan sebagai alat analisis untuk memahami perilaku pelaku kejahatan siber, tetapi juga menjadi landasan dalam merumuskan kebijakan hukum dan sosial yang responsif terhadap perkembangan teknologi dan kompleksitas masyarakat digital.[12]

2. Kerangka Konsepsi

   Adapun dalam penelitian ini, terdapat beberapa konsep sentral yang digunakan untuk mendukung kajian terhadap pertanggungjawaban pidana pelaku kejahatan siber dalam kasus kebocoran Pusat Data Nasional (PDN) tahun 2024. Konsep-konsep tersebut antara lain meliputi: **pertanggungjawaban pidana**, **tindak pidana siber**, dan **kebocoran data elektronik**, yang akan dijelaskan sebagai berikut:

   a. Pertanggungjawaban Pidana
      adalah Pelaku kejahatan memikul akuntabilitas hukum atas perbuatannya, sepanjang tindakan tersebut terbukti secara sah melanggar hukum dan didasari oleh aspek kesalahan yang nyata. Dalam konteks kejahatan siber, pertanggungjawaban pidana ditujukan kepada pelaku yang secara sengaja melakukan serangan digital, seperti peretasan atau penyebaran ransomware, yang menimbulkan kerugian.[13]

   b. Tindak Pidana Siber
      Merupakan Pelanggaran hukum di mana teknologi informasi berperan sentral, baik sebagai instrumen untuk melakukan tindak pidana maupun sebagai sasaran serangannya. Kejahatan siber mencakup aktivitas seperti hacking, phishing, penyebaran malware, dan pencurian data digital. Dalam kasus PDN 2024, tindakan pelaku termasuk dalam kategori kejahatan siber karena menggunakan sistem elektronik untuk melakukan peretasan dan penguncian data.[14]

   c. Kebocoran Data Elektronik
      Suatu kondisi ketika informasi yang seharusnya bersifat rahasia diakses atau disebarluaskan oleh oknum yang tidak punya hak akses. Kebocoran data dapat berlangsung akibat serangan siber, kelalaian pengelola sistem, atau lemahnya infrastruktur keamanan digital. Dampaknya meliputi pelanggaran privasi, kerugian ekonomi, dan menurunnya kepercayaan publik terhadap institusi negara.

   Kerangka teori dan konsepsi ini menjadi dasar dalam melakukan analisis terhadap bentuk pertanggungjawaban pidana pelaku kejahatan siber berdasarkan pendekatan hukum normatif terhadap kasus kebocoran PDN tahun 2024.[15]

---

[12] Soerjono Soekanto, *Sosiologi: Suatu Pengantar*, Jakarta: Rajawali Pers, 2015, hlm. 234–236.

[13] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, (Jakarta: Prenadamedia Group, 2014), hlm. 25–27

[14] Ridwan Arifin, *Hukum Kejahatan Siber: Urgensi Pengaturan dan Penanggulangan Cybercrime di Indonesia*, (Yogyakarta: Deepublish, 2019), hlm. 40–45.

[15] Zainal Abidin Bagir (ed.), *Perlindungan Data Pribadi di Indonesia*, (Jakarta: Komnas HAM, 2020), hlm. 65–70.