(2026), 4 (2): 64–72 **Kultura** 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

PERTANGGUNGJAWABAN PIDANA KORPORASI DALAM KEJAHATAN SIBER DAN TANTANGAN PENEGAKAN HUKUMNYA DI ERA DIGITAL

Novella Ulfa
Progam Studi S1 Ilmu Hukum, FHISIP, Universitas Terbuka

Correspondence
Email: 041711716@ecampus.ut.ac.id No. Telp:
Submitted: 31 March 2026 Accepted: 9 April 2026 Published: 10 April 2026

ABSTRAK

Penelitian ini bertujuan menganalisis konstruksi yuridis pertanggungjawaban pidana korporasi dalam kejahatan siber berdasarkan UU TPPU dan UU ITE; menganalisis tantangan utama dalam penegakan hukum terhadap pertanggungjawaban pidana korporasi dalam kejahatan siber di era digital; serta menganalisis model ideal pertanggungjawaban pidana korporasi dalam kejahatan siber untuk diterapkan dalam sistem hukum Indonesia. Metode penelitian menggunakan pendekatan yuridis normatif. Hasil penelitian menunjukkan konstruksi yuridis telah mengalami evolusi signifikan melalui harmonisasi UU TPPU dan UU ITE. Penegakan hukum terhadap pertanggungjawaban pidana korporasi dalam kejahatan siber di era digital masih menghadapi tantangan multidimensional meliputi: tantangan substantif dan normatif, tantangan prosedural dan pembuktian, tantangan kelembagaan dan koordinasi, tantangan teknologi dan adaptasi hukum, serta tantangan internasional dan kerja sama. Penelitian ini merekomendasikan model ideal pertanggungjawaban pidana korporasi dalam kejahatan siber untuk diterapkan dalam sistem hukum Indonesia melalui model pertanggungjawaban berlapis, sistem sanksi progresif-restoratif, penguatan kelembagaan dengan teknologi forensik digital, mekanisme pencegahan proaktif, dan evaluasi berkelanjutan untuk adaptasi terhadap perkembangan modus kejahatan siber.

Kata Kunci: *era digital, kejahatan siber, korporasi, pertanggungjawaban pidana.*

PENDAHULUAN

Di era digital, pelanggaran data hampir selalu dipahami sebagai peristiwa teknologi (Iskandar, 2026). Transformasi digital yang masif telah mengubah paradigma fundamental dalam ekosistem bisnis dan sosial masyarakat Indonesia, namun di sisi lain menciptakan ruang baru bagi kejahatan siber yang semakin kompleks dan melibatkan entitas korporasi sebagai pelaku utama. Berbagai laporan industry dan studi akademik menunjukkan bahwa insiden siber telah menjadi salah satu ancaman utama dalam pengelolaan risiko korporasi (Gunibala, Maharani, dan Pujiningsih, 2025).

Fenomena kejahatan siber juga mengungkap kompleksitas baru dalam sistem pertanggungjawaban pidana, khususnya ketika korporasi tidak lagi sekedar menjadi korban, melainkan bermetamorfosis menjadi instrumen atau bahkan dalang utama dalam skema kejahatan siber yang merugikan kepentingan publik dan stabilitas ekonomi nasional (Iskandar, 2026). Situasi ini diperparah oleh temuan bahwa mayoritas kasus kejahatan siber korporasi bersinggungan dengan tindak pidana pencucian uang, dimana teknologi digital dimanfaatkan untuk mengaburkan jejak keuangan dan menyulitkan proses penelusuran aset hasil kejahatan (Puannandini, 2021).

Gap penelitian yang mengemuka dalam literatur hukum pidana kontemporer menunjukkan ketidakselarasan antara perkembangan teknologi digital dengan kerangka regulasi pertanggungjawaban pidana korporasi yang masih berkutat pada paradigma konvensional. Penelitian terdahulu cenderung mengkaji pertanggungjawaban pidana korporasi dan kejahatan siber sebagai entitas terpisah, tanpa mengeksplorasi dinamika interseksi keduanya dalam konteks penegakan hukum di era digital. Studi yang dilakukan oleh Pamungkas, Muliyono, dan Lahangatubun (2024) mengidentifikasi krisis penegakan hukum kejahatan siber di Indonesia, namun belum menyentuh aspek fundamental mengenai

bagaimana korporasi sebagai subjek hukum dapat dimintai pertanggungjawaban pidana dalam konteks kejahatan siber yang bersifat transnasional dan virtual.

Demikian pula, riset Widyaningrum, Khoirunnisa, dan Jubaidi (2024) tentang pertanggungjawaban pidana korporasi dalam hukum positif Indonesia masih terbatas pada analisis normatif tanpa mengintegrasikan tantangan spesifik yang muncul dari karakteristik unik kejahatan siber. Kesenjangan ini semakin nyata ketika dikaitkan dengan implementasi UU No. 8 Tahun 2010 tentang TPPU (selanjutnya disingkat UU TPPU) dan UU No. 11 Tahun 2008 tentang ITE serta perubahannya (selanjutnya disingkat UU ITE) yang belum optimal dalam menangani kasus-kasus kompleks yang melibatkan korporasi sebagai subjek kejahatan siber. Saat ini masih ada tantangan dalam implementasi dan penegakan hukum yang efektif (Djibu, 2025: 342).

Aspek *novelty* penelitian ini terletak pada pendekatan interdisipliner yang mengintegrasikan teori pertanggungjawaban pidana korporasi dengan dinamika kejahatan siber dalam kerangka penegakan hukum di era digital, khususnya melalui analisis sinergi antara UU TPPU dan UU ITE sebagai instrumen hukum yang belum pernah dikaji secara komprehensif dalam konteks pertanggungjawaban pidana korporasi. Penelitian ini juga menghadirkan perspektif baru dalam menganalisis efektivitas mekanisme pertanggungjawaban pidana korporasi melalui lensa transformasi digital, dimana konsep tradisional seperti *corporate veil*, *vicarious liability*, dan *corporate culture* perlu diadaptasi untuk mengakomodasi realitas kejahatan siber yang bersifat *virtual* dan *intangible*. Kontribusi teoretis yang ditawarkan adalah formulasi kerangka konseptual baru untuk memahami pertanggungjawaban pidana korporasi dalam dimensi kejahatan siber, yang dapat menjadi landasan bagi pengembangan kebijakan hukum pidana yang lebih responsif terhadap tantangan era digital.

Berdasarkan analisis mendalam terhadap kompleksitas permasalahan yang telah diuraikan, penelitian ini merumuskan beberapa pertanyaan penelitian yang fundamental, yaitu:

1. Bagaimana konstruksi yuridis pertanggungjawaban pidana korporasi dalam kejahatan siber berdasarkan UU TPPU dan UU ITE?
2. Apa saja tantangan utama dalam penegakan hukum terhadap pertanggungjawaban pidana korporasi dalam kejahatan siber di era digital?
3. Bagaimana model ideal pertanggungjawaban pidana korporasi dalam kejahatan siber untuk diterapkan dalam sistem hukum Indonesia?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (*doctrinal research*). Widiarty (2024) menyatakan bahwa "penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti" (p.29). Metode pendekatan yang digunakan dalam penelitian ini adalah kombinasi dari pendekatan perundang-undangan (*statute approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menganalisis secara komprehensif UU TPPU dan UU ITE untuk memahami konstruksi yuridis pertanggungjawaban pidana korporasi. Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum (Widiarty, 2024)

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer berupa UU TPPU dan UU ITE; bahan hukum sekunder meliputi buku-buku hukum, artikel jurnal yang membahas pertanggungjawaban pidana korporasi dan kejahatan siber; serta bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber referensi pendukung lainnya.

Teknik analisis data yang digunakan adalah analisis kualitatif dengan metode deskriptif-analitis dan preskriptif melalui pendekatan *content analysis* untuk menginterpretasikan dan menganalisis bahan hukum yang telah dikumpulkan.

HASIL DAN PEMBAHASAN

Konstruksi Yuridis Pertanggungjawaban Pidana Korporasi dalam Kejahatan Siber Berdasarkan UU TPPU dan UU ITE

Pertanggungjawaban pidana adalah proses pemberian hukuman terhadap pelaku untuk memastikan apakah terdakwa dapat dituntut dalam hal tanggungjawab terhadap perbuatan pidana yang telah dilakukannya (Jaholden, 2021). Korporasi adalah entitas hukum yang dibuat oleh atau di bawah kewenangan hukum untuk bertindak sebagai badan tunggal dan memiliki hak serta kewajiban yang terpisah dari individu-individu yang membentuknya (Purwaningsih, 2025). Konstruksi yuridis pertanggungjawaban pidana korporasi dalam sistem hukum Indonesia telah mengalami evolusi signifikan dengan pengakuan korporasi sebagai subjek hukum pidana. Korporasi diakui sebagai subjek hukum pidana sebagaimana ditegaskan dalam Pasal 45-50 Undang-Undang Nomor 1 tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru), yang memungkinkan badan hukum dikenai pertanggungjawaban pidana (Fadhila, 2024: 653). Konstruksi ini diperkuat oleh Pasal 6 ayat (1) UU TPPU yang menegaskan bahwa apabila tindak pidana pencucian uang dilakukan oleh korporasi, maka pidana dapat dijatuhkan terhadap korporasi dan/atau personil pengendali korporasi.

Chandra (2022) menjelaskan bahwa "subjek hukum pidana tidak hanya manusia, tetapi juga badan hukum" (p.34). Korporasi dapat dimintai pertanggungjawaban ketika tindak pidana dilakukan atas nama, untuk kepentingan, atau melalui mekanisme korporasi. Flora *et.al* (2024) menyatakan bahwa “sistem pemidanaan untuk badan hukum sering kali berbeda dengan individu, dengan fokus pada tanggung jawab perusahaan, rehabilitasi organisasi, dan pencegahan kejahatan korporasi di masa depan” (p.87). Landasan normatif ini semakin kokoh dengan pengaturan dalam UU ITE yang memungkinkan penyelenggara sistem elektronik maupun badan usaha dimintai tanggung jawab pidana bila lalai atau sengaja memungkinkan terjadinya kejahatan siber.

Ruang lingkup kejahatan siber dalam kerangka TPPU mencakup berbagai bentuk *cybercrime* yang dapat menjadi tindak pidana asal (*predicate offence*). Berdasarkan Pasal 2 ayat (1) huruf z UU TPPU, tindak pidana lain yang diancam dengan pidana penjara 4 tahun atau lebih dapat dikualifikasikan sebagai *predicate crime*. Banyak tindak pidana dalam UU ITE memenuhi kriteria tersebut seperti akses ilegal tanpa hak dengan ancaman pidana maksimal 7 tahun penjara, intersepsi tanpa izin dengan ancaman 10 tahun, serta manipulasi data elektronik dengan ancaman 8 tahun. Modus kejahatan siber juga mencakup penyembunyian, transfer, hingga *layering* dana melalui teknologi informasi, dimana korporasi seringkali menjadi kendaraan untuk menyamarkan asal-usul dana.

Kejahatan siber seringkali dilakukan melalui *cyber-dependent crime* dan *cyber-enabled crime*, dimana pencurian data finansial, penggunaan rekening korporasi sebagai *layering* pencucian uang, dan penggunaan teknologi *blockchain* untuk menyamarkan asal-usul dana masuk dalam ruang lingkup TPPU (Puannandini, 2021). Anggun (2022) menjelaskan bahwa "tindak pidana siber kerap menjadi *predicate crime* dalam TPPU" (p.81), seperti *hacking* untuk mencuri data finansial, *phishing* untuk menipu nasabah, atau *ransomware* yang kemudian hasilnya dialirkan ke rekening korporasi. Penelitian Dermawan, Fardiansyah, dan Tamza (2025) menyatakan bahwa kejahatan ekonomi yang dilakukan oleh korporasi di sektor keuangan merupakan fenomena yang semakin kompleks di era digital.

Ketentuan pidana dan sanksi bagi korporasi diatur secara komprehensif dalam Pasal 7 UU TPPU yang menentukan pidana pokok berupa pidana denda paling banyak Rp100.000.000.000,00 (seratus miliar rupiah). Pasal 7 ayat (2) menambahkan pidana tambahan seperti pengumuman putusan hakim, pembekuan sebagian atau seluruh kegiatan usaha, pencabutan izin usaha, pembubaran dan/atau pelarangan korporasi, perampasan aset korporasi, dan pengambilalihan korporasi oleh negara. Hal ini sejalan dengan Pasal 46-47 KUHP Baru. Pasal 9 UU TPPU juga memberikan alternatif pidana pengganti terhadap personil pengendali apabila denda tidak dibayar, menunjukkan skema pemidanaan yang tidak hanya represif terhadap badan hukum, melainkan juga memberikan efek jera bagi pengurus yang bertanggung jawab.

Sinkronisasi UU TPPU dan UU ITE menjadi krusial karena keduanya memiliki peran komplementer dalam menangani kejahatan siber korporasi. UU ITE menetapkan berbagai tindak pidana siber sebagai tindak pidana asal, sementara UU TPPU menyediakan instrumen untuk menjerat hasil kejahatan tersebut agar tidak berputar dalam sistem keuangan. Pentingnya sinkronisasi antara UU ITE dan UU TPPU adalah agar tidak terjadi tumpang tindih penerapan hukum, dengan integrasi yang menghasilkan konstruksi yuridis yang lebih komprehensif. Namun, terdapat tantangan sinkronisasi karena UU ITE dalam banyak ketentuannya menggunakan subjek hukum "setiap orang" tanpa penegasan eksplisit mengenai korporasi sebagai pelaku, sementara UU TPPU secara jelas mengatur pertanggungjawaban korporasi. Penelitian (Firdaus, 2024) mengidentifikasi "*overlapping norms, cross-border jurisdictional constraints*" sebagai kendala sinkronisasi. Penelitian (Wuryandari, 2024) menunjukkan bahwa "regulasi yang ada seperti UU ITE belum sepenuhnya mampu mengakomodasi isu-isu terkini dalam teknologi digital". Kondisi ini menuntut interpretasi progresif dari hakim dan aparat penegak hukum agar korporasi dapat dimintai pertanggungjawaban pidana atas kejahatan siber yang dilakukan untuk kepentingan badan hukum.

Tantangan Penegakan Hukum Pertanggungjawaban Pidana Korporasi dalam Kejahatan Siber di Era Digital

Menurut Efendi, Adinugroho, dan Khomairoh (2025) “tindak pidana konvensional umumnya dapat ditangani dengan metode penegakan hukum konvensional, seperti investigasi lapangan dan penangkapan secara fisik, namun kejahatan siber memerlukan pendekatan yang lebih teknis dan sering kali melibatkan kerja sama internasional karena sifatnya yang lintas batas negara” (p.176). Oleh sebab itu terdapat tantangan penegakan hukum pertanggungjawaban pidana korporasi dalam kejahatan siber di era digital.

Pertama, tantangan substantif dan normatif. Tantangan substantif dan normatif dalam penegakan hukum pidana korporasi kejahatan siber mencakup ketidakjelasan mengenai atribusi perbuatan individu kepada korporasi. Masih terdapat perdebatan teoretis apakah kesalahan individu pengurus otomatis dapat dibebankan kepada korporasi, dengan perbandingan aliran monistis dan dualistis dalam memandang *actus reus* dan *mens rea*. Untuk menetapkan pertanggungjawaban pidana pada korporasi sebagai entitas hukum, diperlukan analisis mendalam mengenai mens rea atau kondisi mental dari korporasi tersebut, yang meliputi sejauh mana kesengajaan atau kelalaiannya. Dalam hal ini, yang diperhatikan bukan hanya *actus reus* (tindakan yang dilakukan), tetapi juga aspek *mens rea* dari korporasi (Nurdipa, dan Zulfiani, 2025). Namun, menentukan *mens rea* dari suatu korporasi seperti bersifat paradoks. Korporasi tidak memiliki ‘pikiran’ nya sendiri layaknya manusia.

Selain itu, perbedaan definisi *cybercrime* antarnegara menciptakan tantangan normatif. Ketidakjelasan ini terutama terjadi ketika perbuatan dilakukan oleh pihak ketiga seperti *vendor* IT atau penyedia jasa *cloud* yang bekerja untuk kepentingan korporasi. Banyak tantangan normatif yang muncul ketika *cybercrime* dapat diungkap oleh aparat penegak

hukum di Indonesia, khususnya apabila dalam kejahatan tersebut terkait unsur-unsur asing, salah satu permasalahan hukum utama yang muncul bersamaan dengan terungkapnya kejahatan tersebut adalah masalah yurisdiksi hukum pidana suatu negara, termasuk kewenangan negara untuk menangkap, menahan, menuntut dan mengadili tersangka (Wahdini, dan Irfansyah, 2024). Kondisi ini menciptakan ketidakpastian hukum yang dapat dimanfaatkan oleh korporasi untuk menghindari pertanggungjawaban pidana.

Kedua, tantangan prosedural dan pembuktian. Tantangan prosedural dan pembuktian menjadi kompleks karena sifat digital *evidence* yang mudah dimanipulasi dan dihapus. Pembuktian aliran dana hasil kejahatan siber sangat sulit karena sifat anonim transaksi digital, termasuk penggunaan *cryptocurrency* (Puannandini, 2021). Pembuktian kesalahan korporasi dalam kejahatan siber sangat rumit karena bukti digital bersifat mudah dihapus, dienkripsi, atau tersebar lintas negara. Meski UU TPPU memperbolehkan informasi elektronik sebagai alat bukti yang sah (Pasal 73), dalam praktiknya keabsahan *log* digital, *metadata*, atau bukti forensik siber masih sering diperdebatkan di pengadilan.

Ketiga, tantangan kelembagaan dan koordinasi. Koordinasi antara PPATK, Kepolisian, Kejaksaan, dan OJK, sering kali belum optimal dalam menangani kasus kejahatan siber korporasi (Dermawan, Fardiansyah, dan Tamza, 2025). Kasus-kasus yang melibatkan instansi negara memperlihatkan bagaimana proses hukum dan administratif berinteraksi, kadang menimbulkan konflik prioritas. Fragmentasi kelembagaan ini menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan siber korporasi untuk menghindari deteksi dan penindakan.

Keempat, tantangan teknologi dan adaptasi hukum. Perkembangan teknologi yang sangat cepat menciptakan kesenjangan antara kemajuan teknologi dan adaptasi hukum. Pelaku siber sering menggunakan teknik enkripsi, *dark web*, dan server luar negeri untuk menyembunyikan jejak kejahatan. Penelitian Marzuki (2025) menunjukkan "transformasi siber yang berlangsung sangat cepat telah membawa berbagai permasalahan baru dalam dunia hukum". Kesenjangan ini memungkinkan korporasi melakukan kejahatan dengan modus baru yang belum terakomodasi dalam regulasi.

Kelima, tantangan internasional dan kerja sama. Karakteristik lintas batas kejahatan siber memerlukan kerjasama internasional yang efektif melalui *mutual legal assistance* dan perjanjian ekstradisi. Penelitian Aditama, Sinaga, dan Putri (2025) mengidentifikasi perbedaan antara negara dalam pendekatan hukum dan strategi penegakannya dalam menangani *cybercrime*. Perbedaan sistem hukum dapat menjadi penghambat ekstradisi dan *mutual legal assistance*. Penelitian Marzuki (2025) juga menunjukkan bahwa harmonisasi hukum internasional masih menghadapi kendala akibat perbedaan sistem hukum dan kebijakan antarnegara. Keterbatasan kerjasama internasional ini memungkinkan korporasi pelaku kejahatan siber berlindung di negara-negara dengan regulasi yang lemah atau tidak memiliki perjanjian ekstradisi.

Model Ideal Pertanggungjawaban Pidana Korporasi dalam Kejahatan Siber untuk Sistem Hukum Indonesia

Reformulasi kerangka normatif memerlukan penegasan eksplisit korporasi sebagai subjek pidana dalam UU ITE melalui revisi atau aturan pelaksana yang merujuk pada prinsip-prinsip Pasal 6 UU TPPU. Diperlukan pembaruan UU ITE dan UU TPPU agar sejalan dengan KUHP baru—melalui ini maka reformulasi dapat menegaskan kedudukan korporasi sebagai subjek pidana yang independen. Model ideal pertanggungjawaban pidana korporasi dalam kejahatan siber untuk sistem hukum Indonesia adalah sebagai berikut:

Pertama, model pertanggungjawaban berlapis (*Layered Accountability*). Model pertanggungjawaban berlapis menempatkan korporasi, personil pengendali, dan unit operasional dalam posisi akuntabilitas yang berbeda namun saling terkait. Purwaningsih

(2025) mengusulkan konsep *layered accountability* menempatkan korporasi, pengurus, dan pemegang saham dalam posisi akuntabilitas berbeda" untuk mencegah "*corporate veil* menjadi alasan impunitas. Chandra (2022) mengusulkan "agar pertanggungjawaban tidak hanya dibebankan kepada korporasi, tetapi juga manajemen dan pemilik modal" dengan "*multi-layered responsibility*". Melalui pendekatan ini korporasi sebagai entitas hukum, pengurus, dan pemilik modal harus sama-sama dapat dimintai pertanggungjawaban. Model ini memungkinkan pemidanaan baik korporasi maupun personil pengendali sebagaimana diatur dalam UU TPPU, memberikan efek ganda dalam pencegahan. Implementasi model ini menghindarkan praktik korporasi yang menggunakan struktur kompleks untuk menghindari pertanggungjawaban pidana. Model berlapis juga memungkinkan penerapan sanksi yang proporsional sesuai dengan tingkat keterlibatan dan tanggung jawab masing-masing pihak dalam struktur korporasi.

Kedua, sistem sanksi progresif dan restoratif**.** Sistem sanksi progresif mengombinasikan denda, remediasi restitusi, dan sanksi restoratif untuk pemulihan korban kejahatan siber. Purwaningsih (2025) menekankan bahwa pemidanaan korporasi harus progresif: dimulai dari denda, pembatasan usaha, hingga pembubaran dengan mekanisme restoratif diperlukan agar sanksi tidak hanya menghukum tetapi juga memperbaiki tata kelola korporasi. Chandra (2022) menekankan integrasi "sanksi progresif—dimulai dari denda administratif hingga pembubaran korporasi—serta mekanisme *restorative justice*". Sistem progresif dimulai dari sanksi administratif, berlanjut ke pidana denda sebagaimana Pasal 7 UU TPPU, kemudian sanksi tambahan seperti pembekuan kegiatan usaha, pencabutan izin, hingga pembubaran korporasi. Aspek restoratif mencakup kewajiban membangun sistem kepatuhan siber, kompensasi kepada korban, dan kerja sama dalam investigasi jaringan kejahatan. Model ini memastikan bahwa sanksi tidak hanya bersifat retributif tetapi juga berkontribusi pada pencegahan dan pemulihan ekosistem digital yang aman (Chandra, 2022).

Ketiga, mekanisme pencegahan dan *early warning system*. Implementasi mekanisme pencegahan proaktif melalui kewajiban *compliance-by-design*, audit elektronik berkala, dan sistem peringatan dini berbasis pemantauan transaksi mencurigakan. Purwaningsih (2025) menekankan urgensi *compliance program* internal perusahaan, misalnya penerapan *Good Corporate Governance* (GCG) yang dihubungkan dengan pencegahan *cybercrime*. Salihi (2024) menekankan pentingnya adaptasi teknologi dalam audit internal guna meningkatkan kualitas pengawasan dan pengendalian di dalam organisasi. Mekanisme pencegahan dapat diperkuat dengan kewajiban pihak pelapor sebagaimana diatur dalam Pasal 17 sampai Pasal 20 UU TPPU untuk menerapkan prinsip *Know Your Customer* (KYC) dalam ekosistem digital. Implementasi *compliance-by-design* memastikan bahwa sistem keamanan siber menjadi bagian integral dari operasional korporasi sejak tahap perencanaan.

Keempat, penguatan kelembagaan dan koordinasi. Model ideal menuntut sinergi antara PPATK dan unit siber Bareskrim Polri yang disertai dengan implementasi teknologi forensik digital mutakhir. Dermawan, Fardiansyah, dan Tamza, (2025) mengusulkan penguatan koordinasi antara PPATK, Kepolisian, Kejaksaan, dan OJK. Penguatan kelembagaan harus mencakup peningkatan kapasitas SDM aparatur dalam bidang teknologi digital, pembentukan unit khusus *cybercrime* di setiap lembaga penegak hukum, dan standardisasi prosedur investigasi lintas lembaga. Koordinasi yang efektif memerlukan sistem informasi terpadu yang memungkinkan *real-time sharing* data dan intelijen antar lembaga. Model ini juga harus mengakomodasi kerjasama dengan sektor swasta, mengingat banyak infrastruktur digital yang dikelola oleh entitas privat.

Kelima, implementasi teknologi dalam penegakan hukum. Pemanfaatan teknologi *artificial intelligence*, *blockchain tracking*, dan *big data analysis* menjadi kunci dalam deteksi pencucian uang berbasis siber dan investigasi kejahatan korporasi. Febriyani, Syarief,

dan Seroja (2024) dalam penelitiannya menekankan potensi pemanfaatan *Artificial Intelligence* dan *big data analysis* menjadi kunci dalam deteksi pencucian uang berbasis siber. Dalam hal ini penggunaan *Artificial Intelligence* untuk *pattern detection*, dan *blockchain analysis* merupakan solusi untuk menembus kerumitan modus korporasi dalam *cybercrime* dimana "tanpa teknologi, aparat akan selalu kalah selangkah dari pelaku".

Keenam, mekanisme evaluasi dan adaptasi berkelanjutan**.** Mekanisme evaluasi berkelanjutan diperlukan agar hukum dapat beradaptasi dengan modus operandi baru dalam kejahatan siber, termasuk memasukkan aset digital seperti *cryptocurrency* secara eksplisit ke dalam rezim TPPU (Puannandini, 2021). Perlu evaluasi periodik regulasi agar tidak tertinggal dari perkembangan teknologi finansial. Hukum pidana korporasi harus dievaluasi secara berkala agar sesuai dengan perkembangan teknologi dengan mekanisme *monitoring* harus bersifat dinamis, agar hukum tidak tertinggal jauh dari modus kejahatan baru. Mekanisme evaluasi harus mencakup *assessment* berkala terhadap efektivitas sanksi, analisis *cost-benefit* kebijakan, dan adaptasi terhadap perkembangan teknologi baru seperti *artificial intelligence*. Sistem evaluasi yang komprehensif memungkinkan identifikasi dini terhadap celah hukum dan penyesuaian regulasi secara proaktif sebelum dieksploitasi oleh pelaku kejahatan korporasi.

KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini mengungkapkan bahwa konstruksi yuridis pertanggungjawaban pidana korporasi dalam kejahatan siber telah mengalami evolusi signifikan dengan pengakuan korporasi sebagai subjek hukum pidana dalam sistem hukum Indonesia, khususnya melalui harmonisasi UU TPPU dan UU ITE. Sinkronisasi kedua regulasi ini menunjukkan peran komplementer dimana UU ITE fokus pada perbuatan kejahatan siber sedangkan UU TPPU menyediakan instrumen untuk menjerat kejahatan pencucian uang yang berasal dari kejahatan siber. Penegakan hukum terhadap pertanggungjawaban pidana korporasi dalam kejahatan siber di era digital masih menghadapi tantangan multidimensional meliputi: tantangan substantif dan normatif; tantangan prosedural dan pembuktian; tantangan kelembagaan dan koordinasi; tantangan teknologi dan adaptasi hukum; serta tantangan internasional dan kerja sama.

Model ideal pertanggungjawaban pidana korporasi dalam kejahatan siber untuk sistem hukum Indonesia adalah sebagai berikut: *Pertama,* model pertanggungjawaban berlapis (*layered accountability*. *Kedua,* sistem sanksi progresif dan restoratif. *Ketiga,* mekanisme pencegahan dan *early warning system*. *Keempat,* penguatan kelembagaan dan koordinasi. *Kelima,* implementasi teknologi dalam penegakan hukum. *Keenam,* mekanisme evaluasi dan adaptasi berkelanjutan.

Saran

Pemerintah Indonesia perlu segera memperbarui dan menyempurnakan regulasi yang ada, seperti UU ITE dan UU TPPU, untuk lebih responsif terhadap perkembangan teknologi digital terkini, termasuk *artificial intelligence* dan *blockchain.* Pemerintah perlu menginvestasikan lebih banyak sumber daya untuk pengembangan kapasitas aparat penegak hukum, khususnya dalam bidang kejahatan siber dan teknologi digital yang dilakukan oleh korporasi.

DAFTAR PUSTAKA

Buku:

Chandra, T.Y. (2022). *Hukum Pidana.* Jakarta: PT. Sangir Multi Usaha.

Flora, H.S., et.al. (2024). *Hukum Pidana Di Era Digital.* Batam: CV. Rey Media Grafika.

Jaholden. (2021). *Reformulasi Hukum Pidana Indonesia*. Deli Serdang: Bircu-Publishing.

Purwaningsih, E. (2025). *Hukum Korporasi*. Kabupaten Purbalingga: Eureka Media Aksara.

Widiarty, W.S. (2024). *Buku Ajar Metode Penelitian Hukum*. Yogyakarta: Publika Global Media.

Jurnal:

Aditama, P., Sinaga, E.A., dan Putri, C.A. (2025). "Perbandingan Hukum Pidana Cyber Crime Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika". *Jurnal Kompilasi Hukum*, 10 (1), 58-76.

Anggun, L. (2022). "Perkembangan Kejahatan Tindak Pidana Pencucian Uang Dan Tindak Pidana Pendanaan Terorisme (TPPU Dan TPPT) Di Masa Pandemi Covid-19". *Technology and Economics Law Journal*, 1(1), 66-83.

Dermawan, R.R., Fardiansyah, A.I., dan Tamza, F.B. (2025). "Analisis Normatif Terhadap Pertanggung Jawaban Pidana Korporasi Dalam Kejahatan Ekonomi Di Sektor Keuangan". *Justicia Sains: Jurnal Ilmu Hukum*, 10 (2), 1013-1024.

Djibu, M.A. (2025). "Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia". *Judge: Jurnal Hukum*, 6(1), 341-347.

Fadhila, K.W. (2024). "Reformasi Hukum Pidana dan Pertanggungjawaban Korporasi dalam UU KUHP 2023". *Action Research Literate*, 8 (3), 649-657.

Febriyani, E., Syarief, E., dan Seroja, T.D. (2024). "Pemanfaatan Artificial Intelligence dalam Deteksi dan Pencegahan Tindak Pidana Pencucian Uang: Potensi dan Tantangan Hukum?". *Jurnal Magister Hukum Udayana*, 13 (4), 877-898.

Gunibala, Z.Y., Maharani, S.N., dan Pujiningsih, S. (2025). "Dampak Finansial Serangan Siber Terhadap Kinerja Korporasi: Scoping Review". *Jurnal Daya Saing*, 11(2), 493-501.

Marzuki, M. (2025). "Urgensi Dunia Hukum Mengejar Kecepatan Transformasi Siber". *Pancasila Law Review*, 2 (1), 1-21.

Nurdipa, I., dan Zulfiani, A. (2025). "Penerapan Doktrin Identifikasi dalam Menentukan Pertanggungjawaban Pidana Korporasi Atas Tindak Pidana Korupsi". *Referendum: Jurnal Hukum Perdata dan Pidana*, 2(2), 104-118.

Pamungkas, A.T., Muliyono, A., dan Lahangatubun, N. (2024). "The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions". *Delictum: Jurnal Hukum Pidana Dan Hukum Pidana Islam*, 2(2), 149–162.

Puannandini, D.A. (2021). "Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency)". *Jurnal Pemuliaan Hukum,* 4(2), 57-70.

Salihi, S.S. (2024). "Peran Teknologi Dalam Meningkatkan Efektivitas Audit Internal". *JITAA: Journal of International Taxation Accounting and Auditing*, 3 (2), 140-148.

Wahdini, S.A.N., dan Irfansyah, F.F.B. (2024). "Analisis Keselarasan Pengaturan Yurisdiksi Cyber Crime dengan Implementasinya di Kehidupan Nyata". *Indonesian Journal of Law and Justice*. 1(3), 1-11.

Widyaningrum, T., Khoirunnisa, K., dan Jubaidi, D. (2024). "Corporate Criminal Liability: An Analysis of Corporate Crime Perpetrators Under Positive Law in Indonesia". *JCH (Jurnal Cendekia Hukum)* 9(2), 146-157.

Website:

Iskandar, Y. (2026, 18 Maret). "Kejahatan Korporasi di Era Digital: Bukan Soal Kebocoran Data, Melainkan Kegagalan dalam Tata Kelola". Diambil dari https://www.hukumonline.com/berita/a/kejahatan-korporasi-di-era-digital--bukan-soal-kebocoran-data--melainkan-kegagalan-dalam-tata-kelola-lt69b9a2bc66285?page=all.