Equality: Law And Social
Volume 2, Nomor 1, 2026
E-ISSN: 3123-1926
Akses Terbuka: https://ejournal.risetanakbangsa.id/jhs

Pertanggungjawaban Pidana Korporasi dalam Kasus Kebocoran Data Pribadi oleh Platform Digital

Ovibrian Sitanggang[1], Muhamad Nur Agik Prastiyo[2], Krisna Sandro Hidayat[3]
[1,2,3] Universitas Pamulang, Indonesia
Korespondensi: brianovi330@email.com

Informasi Artikel

Riwayat artikel:
Diterima Mei 25th, 2026
Direvisi Juni 14th, 2026
Diterima Agustus 02th, 2026

Kata kunci:
Pertanggungjawaban Pidana Korporasi, Platform Digital, Kebocoran Data Pribadi, UU PDP.

ABSTRAK

Penelitian ini membahas pertanggungjawaban pidana korporasi platform digital dalam kasus kebocoran data pribadi di Indonesia. Persoalan ini penting karena kebocoran data tidak lagi sekadar dipandang sebagai pelanggaran administratif, tetapi juga dapat menunjukkan adanya kelalaian sistemik dalam tata kelola korporasi digital. Permasalahan utama terletak pada sulitnya membuktikan unsur kesalahan korporasi ketika kebocoran data terjadi melalui sistem algoritmik, rantai pengolahan data yang kompleks, dan struktur organisasi yang terdesentralisasi. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa UU Perlindungan Data Pribadi, UU ITE, dan KUHP Baru telah membuka ruang pemidanaan terhadap korporasi, tetapi penerapannya masih menghadapi hambatan dalam pembuktian mens rea, hubungan kausalitas, dan standar kelalaian korporasi. Ketiadaan standar teknis keamanan data yang mengikat menyebabkan aparat penegak hukum kesulitan menentukan batas antara kegagalan teknis biasa dan kelalaian pidana. Diperlukan rekonstruksi kebijakan pidana melalui penguatan standar keamanan siber, audit kepatuhan, dan pengakuan terhadap konsep kelalaian digital korporasi. Reformulasi ini penting untuk menciptakan kepastian hukum, perlindungan data pribadi yang efektif, serta efek jera bagi platform digital.

PENDAHULUAN

Perkembangan teknologi digital telah melahirkan ekosistem ekonomi baru yang didominasi oleh platform digital sebagai pengumpul, penyimpan, dan pengolah data pribadi dalam skala masif. Data pribadi yang pada era ekonomi digital telah menjadi komoditas strategis tidak hanya memiliki nilai ekonomi, tetapi juga mengandung risiko hukum yang besar apabila tidak dikelola secara aman dan bertanggung jawab. Salah satu risiko yang paling menonjol adalah terjadinya kebocoran data pribadi atau data breach yang dapat menimbulkan kerugian bagi konsumen, baik secara ekonomi, sosial, maupun psikologis, serta berpotensi memenuhi unsur tindak pidana apabila terjadi karena kesengajaan, kelalaian serius, atau kegagalan korporasi dalam memenuhi kewajiban perlindungan data. Fenomena ini menempatkan korporasi digital pada posisi sentral sebagai entitas yang menguasai infrastruktur teknologi, sistem pengelolaan data, dan mekanisme pengambilan keputusan berbasis digital. Oleh karena itu, diperlukan konstruksi hukum pidana yang mampu menjangkau pertanggungjawaban korporasi secara utuh, khususnya dalam konteks kebocoran data pribadi pada platform digital. Wijaya menegaskan bahwa penyedia layanan teknologi informasi berbasis web dan aplikasi memiliki potensi besar untuk dimintai pertanggungjawaban pidana karena posisinya sebagai pengendali data yang secara langsung mengelola informasi pribadi pengguna (Wijaya, 2021).

Dalam sistem hukum pidana Indonesia, tradisi pemidanaan selama ini cenderung berorientasi pada individu atau natuurlijk persoon, sedangkan korporasi atau rechtspersoon kerap dipandang sebagai subjek hukum yang sulit dimintai pertanggungjawaban pidana secara mandiri. Padahal, dalam kasus kebocoran data pribadi oleh platform digital, sumber terjadinya pelanggaran tidak selalu berasal dari tindakan individu tertentu, melainkan dapat berakar pada kebijakan internal korporasi, lemahnya sistem keamanan siber, kelalaian pengawasan manajemen, desain sistem yang tidak aman, hingga orientasi bisnis yang lebih mengutamakan keuntungan ekonomi dibandingkan perlindungan hak pengguna. Dalam konteks ini, pertanggungjawaban pidana korporasi memerlukan pergeseran paradigma dari

pendekatan individualistik menuju pengakuan bahwa korporasi dapat memiliki kesalahan atau mens rea yang bersifat independen dari pengurusnya (Priyatno, 2017). Pergeseran paradigma tersebut menjadi penting karena struktur korporasi modern, khususnya korporasi digital, tidak lagi sederhana, melainkan telah berkembang menjadi entitas kompleks dengan sistem kerja, pengambilan keputusan, dan pengelolaan risiko yang terdistribusi.

Beberapa penelitian terdahulu telah mengkaji pertanggungjawaban hukum atas kebocoran data pribadi di Indonesia. Penelitian Wijaya menitikberatkan pada tanggung jawab penyelenggara sistem elektronik terhadap perlindungan data pengguna (Wijaya, 2021). Simanjuntak dan Waluyo mengkaji pertanggungjawaban pidana dalam serangan ransomware terhadap penyedia layanan digital, khususnya dalam kaitannya dengan perlindungan data pribadi dan keamanan sistem elektronik (Simanjuntak & Waluyo, 2025). Sementara itu, Panjaitan membahas aspek normatif pertanggungjawaban korporasi dalam tindak pidana siber, terutama dalam kerangka hukum pidana korporasi dan kejahatan berbasis teknologi informasi (Panjaitan, 2022).

Meskipun demikian, penelitian-penelitian tersebut pada umumnya masih berfokus pada konsep pertanggungjawaban korporasi dalam kerangka hukum konvensional dan belum secara khusus mengkaji bagaimana konsep kesalahan pidana korporasi diterapkan terhadap platform digital yang menggunakan sistem algoritmik, kecerdasan buatan, big data, dan struktur pengambilan keputusan yang terdesentralisasi. Padahal, karakteristik teknologi digital modern telah menciptakan tantangan baru dalam pembuktian unsur kesalahan dan hubungan kausalitas dalam tindak pidana kebocoran data pribadi. Dalam sistem digital yang berbasis algoritma, keputusan atau kegagalan sistem tidak selalu dapat ditelusuri secara langsung kepada satu orang pengurus atau pegawai tertentu. Kesalahan dapat muncul dari akumulasi keputusan korporasi, desain teknologi, kebijakan keamanan yang tidak memadai, pembiaran terhadap risiko, atau kegagalan dalam menerapkan prinsip kehati-hatian dalam pemrosesan data pribadi.

Berdasarkan kondisi tersebut, terdapat research gap berupa belum adanya kajian komprehensif mengenai rekonstruksi konsep pertanggungjawaban pidana korporasi terhadap kegagalan sistem algoritmik dalam platform digital. Kekosongan kajian ini penting untuk diisi karena model pertanggungjawaban pidana korporasi yang masih bertumpu pada identifikasi kesalahan individu berpotensi tidak memadai dalam menjangkau kejahatan atau pelanggaran yang lahir dari sistem korporasi digital yang kompleks. Oleh karena itu, penelitian ini berupaya mengisi kekosongan tersebut melalui analisis normatif terhadap konsep corporate criminal liability dalam konteks perlindungan data pribadi di Indonesia.

Secara normatif, Indonesia telah memiliki sejumlah instrumen hukum yang dapat menjadi dasar dalam menjerat korporasi dalam perkara kebocoran data pribadi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya mengatur mengenai perlindungan data pribadi dalam penyelenggaraan sistem elektronik. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi secara lebih khusus mengatur kewajiban pengendali data pribadi dan prosesor data pribadi, termasuk tanggung jawab hukum atas pemrosesan data pribadi yang tidak sesuai dengan ketentuan peraturan perundang-undangan. UU PDP juga memberikan ruang bagi pemidanaan terhadap korporasi sebagai subjek hukum apabila terjadi pelanggaran terhadap ketentuan perlindungan data pribadi. Pengaturan tersebut diperkuat oleh Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengatur kewajiban penyelenggara sistem elektronik dalam menjamin keamanan, keandalan, dan tanggung jawab terhadap sistem elektronik yang dikelolanya. Simanjuntak dan Waluyo mencatat bahwa perkembangan hukum positif Indonesia menunjukkan adanya kecenderungan penguatan posisi korporasi sebagai subjek hukum pidana yang dapat dimintai pertanggungjawaban atas kebocoran data pribadi yang terjadi dalam sistem digital (Simanjuntak & Waluyo, 2025).

Kebaruan penelitian ini terletak pada upaya merekonstruksi konsep pertanggungjawaban pidana korporasi berdasarkan pendekatan aggregation theory dan collective corporate knowledge dalam konteks platform digital berbasis algoritma. Berbeda dengan penelitian sebelumnya yang masih berorientasi pada konsep traditional corporate liability, penelitian ini menawarkan model pertanggungjawaban yang lebih adaptif terhadap perkembangan kecerdasan buatan, big data, dan sistem pengambilan keputusan digital yang terdesentralisasi. Melalui pendekatan tersebut, kesalahan korporasi tidak hanya dilihat dari tindakan satu individu tertentu, tetapi juga dari akumulasi pengetahuan, kebijakan, keputusan, pembiaran, dan kegagalan sistemik yang terjadi dalam struktur korporasi digital.

Urgensi penelitian ini semakin kuat karena kebocoran data pribadi pada platform digital tidak lagi dapat dipandang sebagai persoalan administratif atau perdata semata, melainkan telah berkembang menjadi persoalan hukum pidana yang berdampak luas terhadap hak privasi, keamanan ekonomi, kepercayaan publik, dan stabilitas ekosistem digital nasional. Ketika platform digital mengelola data pribadi dalam jumlah besar melalui sistem algoritmik dan kecerdasan buatan, kegagalan perlindungan data tidak selalu dapat ditelusuri hanya kepada kesalahan individu tertentu, melainkan dapat bersumber dari kebijakan korporasi, desain sistem, kelalaian pengawasan, budaya organisasi, atau pembiaran terhadap risiko keamanan digital. Oleh karena itu, rekonstruksi pertanggungjawaban pidana korporasi menjadi penting agar hukum pidana mampu menjangkau bentuk kesalahan kolektif dalam korporasi digital, khususnya ketika terjadi kebocoran data yang merugikan konsumen dan melemahkan kepercayaan masyarakat terhadap transformasi digital (Priyatno, 2017; Wijaya, 2021). Urgensi tersebut juga sejalan dengan kebutuhan pembaruan hukum pidana nasional yang tidak hanya bersifat represif setelah terjadinya pelanggaran, tetapi juga preventif dalam mendorong korporasi digital untuk membangun sistem perlindungan data yang aman, transparan, akuntabel, dan sesuai dengan prinsip perlindungan hak subjek data (Simanjuntak & Waluyo, 2025).

Berdasarkan latar belakang permasalahan yang telah diuraikan, penelitian ini difokuskan pada tiga aspek utama. Pertama, penelitian ini mengkaji konstruksi pertanggungjawaban pidana korporasi dalam kasus kebocoran data pribadi yang dilakukan atau terjadi pada platform digital berdasarkan hukum positif Indonesia, khususnya yang diatur dalam Undang-Undang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta ketentuan dalam Kitab Undang-Undang Hukum Pidana yang baru. Kedua, penelitian ini menganalisis berbagai problematika yang muncul dalam pembuktian unsur kesalahan korporasi, terutama ketika kebocoran data pribadi terjadi akibat kegagalan sistem algoritmik, penggunaan teknologi kecerdasan buatan, maupun struktur organisasi digital yang terdesentralisasi sehingga menyulitkan identifikasi pihak yang bertanggung jawab secara langsung. Ketiga, penelitian ini berupaya merumuskan formulasi kebijakan hukum pidana yang ideal guna memperkuat sistem pertanggungjawaban pidana korporasi dalam perlindungan data pribadi.

Dengan demikian, penelitian ini memiliki urgensi akademik dan praktis dalam memperkuat konsep pertanggungjawaban pidana korporasi di era digital. Secara akademik, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan teori pertanggungjawaban pidana korporasi yang lebih sesuai dengan karakteristik platform digital modern. Secara praktis, penelitian ini diharapkan dapat memberikan arah bagi pembentuk undang-undang, aparat penegak hukum, dan penyelenggara platform digital dalam membangun sistem hukum pidana yang lebih responsif, adaptif, dan efektif dalam memberikan perlindungan terhadap data pribadi masyarakat. Hal ini penting agar perkembangan teknologi digital tidak hanya mendorong pertumbuhan ekonomi, tetapi juga berjalan seiring dengan kepastian hukum, keadilan, akuntabilitas korporasi, dan perlindungan hak-hak warga negara.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan spesifikasi deskriptif-analitis, karena fokus kajiannya diarahkan pada analisis norma hukum, asas hukum, doktrin, dan konstruksi pertanggungjawaban pidana korporasi dalam kasus kebocoran data pribadi pada platform digital. Penelitian hukum normatif bertumpu pada bahan hukum primer, sekunder, dan tersier sebagai dasar analisis hukum (Marzuki, 2017). Pendekatan yang digunakan meliputi pendekatan perundang-undangan untuk menelaah konsistensi pengaturan dalam Undang-Undang Pelindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta KUHP Baru; pendekatan konseptual untuk mengkaji doktrin pertanggungjawaban pidana korporasi atau *corporate criminal liability* sebagaimana dikembangkan dalam hukum pidana korporasi (Priyatno, 2017; Widodo, 2009); pendekatan kasus untuk menelaah relevansi putusan pengadilan, antara lain Putusan PN Sleman Nomor 527/Pid.Sus/2020/PN Smn, serta berbagai kasus kebocoran data yang terjadi di Indonesia; dan pendekatan perbandingan guna memperkaya analisis melalui perbandingan model pertanggungjawaban pidana korporasi di yurisdiksi lain (Qamar & Rezah, 2020; McPeak, 2021).

Bahan hukum primer dan sekunder dianalisis dengan teknik interpretasi sistematis dan teleologis untuk menemukan hubungan antaraturan, ratio legis, serta arah kebijakan hukum pidana yang lebih adaptif terhadap perkembangan teknologi digital dan platform berbasis algoritma. Melalui metode tersebut, penelitian ini bertujuan untuk mengonstruksi ulang konsep kesalahan korporasi agar mampu

menjangkau karakteristik platform digital yang bekerja melalui sistem algoritmik, pengolahan data berskala besar, dan relasi hukum antara korporasi digital dengan pengguna. Selain itu, penelitian ini juga bertujuan untuk menganalisis kendala pembuktian dalam penerapan Pasal 73 UU PDP dan Pasal 45A UU ITE, terutama berkaitan dengan pembuktian unsur kesalahan, hubungan antara tindakan pengurus dan korporasi, serta posisi korporasi sebagai pengendali data pribadi, sebagaimana juga menjadi perhatian dalam kajian mengenai praktik pembuktian tindak pidana berbasis teknologi di Indonesia (Panjaitan, 2022; Wijaya, 2021).

HASIL DAN PEMBAHASAN

Rekonstruksi Doktrin Pertanggungjawaban Pidana Korporasi terhadap Kegagalan Sistem Algoritmik dan Struktur Desentralisasi Platform Digital

Pembahasan utama dalam isu ini terletak pada kesulitan mempertemukan konsep klasik *mens rea* dengan struktur korporasi digital yang semakin kompleks. Platform digital tidak lagi beroperasi melalui struktur komando tunggal, melainkan melalui algoritma otonom, *cloud computing*, *data processor* pihak ketiga, dan sistem pengambilan keputusan berbasis data. Dalam konteks ini, muncul persoalan apakah kesalahan korporasi tetap dapat diidentifikasi ketika kebocoran data disebabkan oleh kegagalan sistem algoritmik yang tidak secara langsung mencerminkan niat jahat dewan direksi. Pendekatan *doctrine of identification* yang menitikberatkan kesalahan pada pengurus puncak atau *directing mind* menjadi sulit diterapkan pada korporasi digital yang memiliki struktur terdesentralisasi dan lintas yurisdiksi (Priyatno, 2017; Mcpeak, 2021).

Doktrin identifikasi berangkat dari asumsi bahwa tindakan dan sikap batin individu tertentu yang memiliki otoritas pengendali dalam korporasi dapat dipandang sebagai tindakan dan sikap batin korporasi itu sendiri. Namun, dalam praktik platform digital modern, keputusan operasional kerap dilakukan oleh manajer tingkat menengah, insinyur perangkat lunak, analis data, atau bahkan sistem otomatis berbasis kecerdasan buatan. Kondisi ini melahirkan *problem of many hands*, yaitu keadaan ketika kesalahan tersebar pada banyak aktor sehingga sulit menunjuk satu pihak sebagai *directing mind* yang mewakili kesalahan korporasi (Mcpeak, 2021).

Keterbatasan doktrin identifikasi menunjukkan bahwa model pertanggungjawaban pidana korporasi perlu bergeser dari pendekatan individualistik menuju pendekatan organisasional. Kesalahan korporasi tidak semata-mata harus dicari pada kehendak pengurus puncak, tetapi dapat ditemukan dalam pola kebijakan, budaya kepatuhan, kelemahan tata kelola, dan pembiaran sistemik terhadap risiko keamanan data. Dalam konteks kebocoran data pribadi, kegagalan membangun sistem keamanan yang memadai, mengabaikan hasil audit keamanan, atau menunda perbaikan kerentanan sistem dapat dipandang sebagai bentuk kesalahan korporasi yang bersifat struktural (Panjaitan, 2022).

Sebagai alternatif, doktrin pengetahuan kolektif atau *aggregation theory* lebih adaptif untuk menjangkau karakter korporasi digital. Doktrin ini memungkinkan pengadilan menggabungkan pengetahuan, keputusan, dan kelalaian dari beberapa organ internal korporasi untuk membentuk satu kesatuan *mens rea* korporasi. Misalnya, apabila divisi keamanan informasi telah mengetahui adanya kerentanan sistem, divisi keuangan menolak alokasi anggaran perbaikan, dan divisi pemasaran tetap mengumpulkan data sensitif pengguna, maka secara kolektif korporasi dapat dianggap mengetahui risiko kebocoran data namun tetap membiarkannya terjadi (Priyatno, 2017; Mcpeak, 2021).

Problematika berikutnya terletak pada ranah pembuktian. Kebocoran data pribadi tidak selalu lahir dari kesengajaan (*dolus*), tetapi juga dapat disebabkan oleh kelalaian berat (*culpa lata*) dalam menerapkan prinsip *privacy by design* dan *privacy by default*. Pembuktian kelalaian memerlukan standar objektif untuk menilai apakah korporasi telah melakukan langkah pencegahan yang wajar dan memadai. UU PDP memang mensyaratkan kewajiban pengendali data pribadi untuk menjaga keamanan data, tetapi standar "memadai" dalam perlindungan data pribadi masih belum sepenuhnya dirumuskan secara teknis dalam peraturan pelaksana (Panjaitan, 2022; Anggraeni and Partners, 2025).

Aparat penegak hukum juga menghadapi kesulitan dalam membuktikan hubungan kausal antara kebijakan makro korporasi dan akibat konkret berupa kebocoran data. Misalnya, keputusan pemotongan anggaran keamanan siber dapat berkontribusi terhadap lemahnya sistem pertahanan digital, tetapi belum tentu mudah dibuktikan sebagai penyebab langsung dari keberhasilan serangan *ransomware*. Dalam hukum pidana, hubungan kausalitas harus menunjukkan keterkaitan yang cukup kuat antara perbuatan, kelalaian, dan akibat. Namun, dalam ekosistem digital, kebocoran data sering

merupakan hasil dari rangkaian peristiwa yang melibatkan bug perangkat lunak, kesalahan manusia, kelemahan konfigurasi sistem, dan serangan eksternal secara bersamaan (Mcpeak, 2021).

Ketiadaan standar audit keamanan siber yang diakui secara tegas sebagai standar kehati-hatian minimum memperbesar ruang pembelaan bagi korporasi. Korporasi dapat berargumentasi bahwa kebocoran data merupakan peristiwa yang tidak dapat dihindari (*unavoidable accident*) karena serangan dilakukan oleh pihak ketiga dengan teknologi canggih. Oleh karena itu, diperlukan konstruksi hukum yang menempatkan standar kepatuhan keamanan digital sebagai indikator objektif untuk menilai ada atau tidaknya kelalaian korporasi. Standar tersebut dapat mencakup audit berkala, enkripsi data, pembatasan akses internal, pencatatan insiden, pelaporan kebocoran, dan evaluasi risiko secara berkelanjutan (Panjaitan, 2022).

Jika merujuk pada UU PDP dan UU ITE, masih terdapat kesenjangan normatif dalam pengaturan sanksi pidana terhadap korporasi digital. UU PDP telah membuka ruang penjatuhan pidana denda terhadap korporasi, tetapi belum secara eksplisit mengatur pidana tambahan seperti pembubaran korporasi atau pencabutan izin operasional untuk kategori kegagalan sistemik perlindungan data. Panjaitan menilai bahwa masih terdapat kekosongan hukum dalam membedakan tindak pidana yang dilakukan oleh pengurus dengan tindak pidana yang bersumber dari kegagalan sistem korporasi sebagai entitas (Panjaitan, 2022).

Dalam praktik penegakan hukum di Indonesia, pertanggungjawaban pidana korporasi digital juga belum berkembang secara optimal. Putusan Pengadilan Negeri Sleman Nomor 527/Pid.Sus/2020/PN Smn masih menunjukkan pola pemidanaan yang berorientasi pada individu, bukan pada korporasi sebagai subjek hukum mandiri. Hal ini memperlihatkan bahwa meskipun korporasi secara normatif dapat dipidana, praktik penegakan hukum masih cenderung menjadikan pengurus teknis atau pelaku individual sebagai titik utama pertanggungjawaban. Akibatnya, korporasi yang memperoleh manfaat dari pengolahan data tetap berpotensi terhindar dari pertanggungjawaban pidana yang proporsional (Priyatno, 2017; Panjaitan, 2022).

Fakta empiris menunjukkan bahwa kasus kebocoran data pribadi di Indonesia lebih sering diselesaikan melalui mekanisme administratif dibandingkan mekanisme pidana. Anggraeni and Partners mencatat bahwa penegakan UU PDP, termasuk dalam kasus kebocoran data Bank Syariah Indonesia, masih didominasi oleh sanksi administratif yang dijatuhkan oleh otoritas terkait, sementara belum terdapat putusan pengadilan yang secara tegas menjatuhkan sanksi pidana terhadap korporasi digital (Anggraeni and Partners, 2025). Pola serupa terlihat dalam kasus kebocoran 279 juta data penduduk BPJS Kesehatan pada tahun 2021 dan kebocoran 204 juta data Daftar Pemilih Tetap Pemilu 2024 milik KPU, yang penanganannya lebih menitikberatkan pada pelaku peretasan dibandingkan pertanggungjawaban kelembagaan pengendali data (Chaterine & Prabowo, 2021; Dwi, 2023; Simanjuntak & Waluyo, 2025).

Secara akademis, masih terdapat perdebatan mengenai apakah model pertanggungjawaban pidana korporasi di Indonesia lebih dekat pada *vicarious liability* atau *corporate liability* murni. Priyatno membedakan keduanya berdasarkan letak kesalahan, yaitu apakah kesalahan melekat pada pengurus lalu dibebankan kepada korporasi, atau korporasi dipandang memiliki kesalahan sendiri sebagai entitas hukum (Priyatno, 2017). KUHP Baru memang mengakui korporasi sebagai subjek tindak pidana, tetapi rumusan bahwa tindak pidana dilakukan "oleh pengurus, untuk dan atas nama korporasi" masih menyisakan masalah ketika tindakan dilakukan oleh developer tingkat menengah, sistem otomatis, atau algoritma tanpa pengetahuan langsung direksi (Mcpeak, 2021).

Oleh karena itu, rekonstruksi doktrin pertanggungjawaban pidana korporasi terhadap platform digital perlu diarahkan pada konsep *organizational fault* atau kesalahan organisasional. Dalam model ini, kesalahan korporasi tidak hanya dilihat dari tindakan pengurus puncak, tetapi dari kegagalan korporasi membangun sistem kepatuhan, pengawasan algoritmik, tata kelola keamanan data, dan mekanisme mitigasi risiko. Dengan pendekatan tersebut, korporasi dapat dimintai pertanggungjawaban apabila terbukti memperoleh manfaat dari pemrosesan data, mengetahui atau seharusnya mengetahui adanya risiko, tetapi gagal mengambil langkah pencegahan yang layak (Priyatno, 2017; Panjaitan, 2022; Mcpeak, 2021).

Rekonstruksi tersebut juga penting untuk mencegah penggunaan struktur desentralisasi sebagai alat menghindari tanggung jawab pidana. Korporasi digital tidak boleh berlindung di balik kompleksitas algoritma, rantai vendor, atau pembagian fungsi internal untuk meniadakan kesalahan. Justru semakin besar skala pemrosesan data dan semakin tinggi ketergantungan pada teknologi otomatis, semakin besar

pula kewajiban korporasi untuk memastikan adanya pengawasan manusia, audit keamanan, dokumentasi keputusan, dan sistem akuntabilitas yang dapat diuji secara hukum. Dengan demikian, hukum pidana dapat berfungsi tidak hanya sebagai instrumen penghukuman, tetapi juga sebagai sarana mendorong tata kelola platform digital yang aman, transparan, dan bertanggung jawab.

Model Ideal Pertanggungjawaban Pidana Korporasi Digital dalam Perlindungan Data Pribadi di Indonesia

Berdasarkan uraian mengenai rekonstruksi doktrin dan perbandingan pengaturan di beberapa negara, model ideal pertanggungjawaban pidana korporasi digital di Indonesia perlu diarahkan pada pendekatan yang lebih komprehensif, sistemik, dan berbasis risiko. Pertanggungjawaban pidana korporasi tidak lagi cukup apabila hanya dibangun melalui pembuktian kesalahan individu tertentu dalam struktur perusahaan. Dalam praktik platform digital, kebocoran data pribadi sering kali terjadi bukan karena satu tindakan tunggal, melainkan akibat kegagalan sistem keamanan, lemahnya pengawasan internal, tidak optimalnya audit teknologi informasi, serta pembiaran terhadap risiko yang telah diketahui sebelumnya. Oleh karena itu, model pertanggungjawaban pidana korporasi perlu menempatkan korporasi sebagai subjek hukum yang memiliki kewajiban aktif untuk mencegah, mengendalikan, dan memitigasi risiko kebocoran data pribadi (Widodo, 2009; Priyatno, 2017; Arief & Purwanto, 2025).

Model ideal tersebut dapat dibangun melalui penguatan konsep kesalahan organisasional. Dalam konsep ini, kesalahan korporasi tidak hanya dinilai dari ada atau tidaknya niat jahat pengurus, tetapi juga dari kualitas tata kelola internal, budaya kepatuhan, kebijakan keamanan data, serta kemampuan korporasi dalam merespons risiko siber. Apabila korporasi telah mengetahui atau seharusnya mengetahui adanya potensi kebocoran data, tetapi tidak melakukan langkah pencegahan yang layak, maka kelalaian tersebut dapat dipandang sebagai bentuk kesalahan pidana korporasi. Dengan demikian, pembuktian kesalahan tidak semata-mata diarahkan pada individu, tetapi pada kegagalan korporasi sebagai organisasi dalam memenuhi standar kehati-hatian digital (Priyatno, 2017; Mcpeak, 2021).

Penguatan pertanggungjawaban pidana korporasi digital juga perlu disertai dengan penetapan parameter objektif mengenai standar keamanan data pribadi. Parameter tersebut dapat meliputi kewajiban audit keamanan secara berkala, penerapan enkripsi data, pembatasan akses internal, dokumentasi aktivitas pemrosesan data, pelaporan insiden kebocoran, serta evaluasi risiko terhadap sistem elektronik yang digunakan. Keberadaan parameter yang jelas akan membantu aparat penegak hukum dalam menilai apakah suatu korporasi telah menjalankan kewajiban perlindungan data secara memadai atau justru lalai dalam membangun sistem keamanan. Tanpa standar yang objektif, pembuktian kelalaian korporasi akan terus menghadapi hambatan karena korporasi dapat berdalih bahwa kebocoran data terjadi akibat serangan pihak ketiga yang berada di luar kendalinya (Akila & Lukitasari, 2024; Arief & Purwanto, 2025).

Selain aspek pembuktian, model ideal pertanggungjawaban pidana korporasi juga perlu memperkuat hubungan antara sanksi administratif dan sanksi pidana. Dalam banyak kasus kebocoran data, penyelesaian melalui sanksi administratif memang penting sebagai mekanisme korektif dan preventif. Namun, apabila kebocoran data terjadi secara masif, berulang, melibatkan data sensitif, atau disebabkan oleh kelalaian berat korporasi, maka instrumen pidana perlu digunakan sebagai bentuk pertanggungjawaban yang lebih tegas. Sanksi pidana terhadap korporasi tidak hanya berfungsi sebagai pembalasan, tetapi juga sebagai sarana untuk mendorong korporasi membangun sistem kepatuhan yang lebih kuat dan bertanggung jawab (UU Nomor 27 Tahun 2022; PERMA Nomor 13 Tahun 2016).

Dalam konteks kebijakan hukum pidana, penguatan model pertanggungjawaban korporasi digital dapat dilakukan melalui pembaruan norma yang secara tegas mengatur kelalaian korporasi dalam perlindungan data pribadi. Norma tersebut perlu menjelaskan bahwa korporasi dapat dimintai pertanggungjawaban apabila kegagalan perlindungan data disebabkan oleh lemahnya sistem pengawasan, tidak dipenuhinya standar keamanan minimum, atau pembiaran terhadap kerentanan sistem yang telah diketahui. Pengaturan ini penting agar hukum pidana tidak hanya menindak pelaku peretasan secara individual, tetapi juga dapat menjangkau korporasi yang memperoleh manfaat ekonomi dari pengolahan data namun gagal melindungi hak subjek data pribadi (Wijaya, 2021; Arief & Purwanto, 2025).

Model ideal tersebut juga perlu menempatkan prinsip kehati-hatian digital sebagai standar utama dalam menilai tanggung jawab korporasi. Prinsip ini mengharuskan setiap korporasi digital untuk tidak hanya bereaksi setelah terjadi kebocoran data, tetapi sejak awal membangun sistem pencegahan yang memadai. Dalam konteks ini, kewajiban korporasi tidak terbatas pada penyediaan sistem elektronik, melainkan juga mencakup pengawasan terhadap pihak ketiga, pelatihan sumber daya manusia, pembentukan unit kepatuhan data pribadi, serta penyusunan prosedur tanggap insiden. Apabila korporasi mengabaikan kewajiban tersebut, maka kelalaiannya dapat dikualifikasikan sebagai kegagalan struktural yang berimplikasi pada pertanggungjawaban pidana korporasi (Akila & Lukitasari, 2024; Alkarmi, Sarabi, & Liu, 2026).

Selain itu, model pertanggungjawaban pidana korporasi digital perlu memperhatikan kedudukan korban sebagai subjek data pribadi. Kebocoran data tidak hanya menimbulkan kerugian ekonomi, tetapi juga dapat mengancam privasi, keamanan, reputasi, dan hak konstitusional warga negara. Oleh karena itu, pendekatan pemidanaan terhadap korporasi digital harus diarahkan tidak hanya pada penghukuman, tetapi juga pada pemulihan kerugian korban. Bentuk pemulihan tersebut dapat berupa pemberitahuan kepada korban, penyediaan mekanisme pengaduan, kompensasi yang layak, pemulihan akses, serta perbaikan sistem keamanan agar peristiwa serupa tidak berulang. Dengan demikian, pertanggungjawaban pidana korporasi digital harus memiliki orientasi perlindungan korban dan pemulihan kepercayaan publik terhadap ekosistem digital (UU Nomor 27 Tahun 2022; Alkarmi et al., 2026).

Selanjutnya, diperlukan pula penguatan kapasitas aparat penegak hukum dalam menangani perkara kebocoran data yang melibatkan korporasi digital. Kompleksitas pembuktian dalam perkara siber menuntut kemampuan teknis untuk memahami jejak digital, sistem algoritmik, audit keamanan informasi, serta hubungan hukum antara pengendali data, prosesor data, dan pihak ketiga. Tanpa dukungan keahlian digital forensik dan pemahaman terhadap tata kelola teknologi informasi, penegakan hukum pidana terhadap korporasi digital berpotensi hanya berhenti pada pelaku teknis atau individu tertentu. Oleh karena itu, model ideal pertanggungjawaban pidana korporasi digital harus didukung oleh mekanisme pembuktian yang adaptif, kolaborasi dengan ahli teknologi informasi, serta pedoman penanganan perkara yang secara khusus mengatur kejahatan korporasi dalam ekosistem digital (PERMA Nomor 13 Tahun 2016; Mcpeak, 2021).

Dalam perspektif pembaruan hukum pidana nasional, keberadaan KUHP Baru dan Undang-Undang Perlindungan Data Pribadi perlu diharmonisasikan agar tidak terjadi kekosongan maupun tumpang tindih pengaturan. Harmonisasi ini penting karena pertanggungjawaban pidana korporasi dalam perlindungan data pribadi berada pada persimpangan antara hukum pidana, hukum administrasi, hukum teknologi informasi, dan hukum perlindungan konsumen. Apabila norma pidana tidak dirumuskan secara jelas, maka aparat penegak hukum akan kesulitan menentukan batas antara pelanggaran administratif biasa dan kelalaian berat yang layak dipidana. Oleh sebab itu, diperlukan formulasi norma yang tegas mengenai kriteria kesalahan korporasi, standar minimum keamanan data, bentuk kelalaian yang dapat dipidana, serta jenis sanksi yang proporsional terhadap tingkat kerugian dan risiko yang ditimbulkan (Widodo, 2009; Priyatno, 2017; Arief & Purwanto, 2025).

Dengan demikian, model ideal pertanggungjawaban pidana korporasi digital di Indonesia harus dibangun melalui kombinasi antara kesalahan organisasional, standar keamanan berbasis risiko, penguatan pembuktian kelalaian, perlindungan korban, serta integrasi antara sanksi administratif dan pidana. Pendekatan ini penting agar hukum pidana mampu menjawab tantangan kebocoran data pribadi dalam ekosistem digital yang kompleks. Melalui model tersebut, korporasi digital tidak dapat lagi berlindung di balik struktur organisasi yang terdesentralisasi, sistem algoritmik, atau keterlibatan pihak ketiga untuk menghindari tanggung jawab. Sebaliknya, semakin besar skala pengolahan data yang dilakukan oleh korporasi, semakin besar pula kewajiban hukumnya untuk memastikan perlindungan data pribadi masyarakat secara aman, transparan, dan akuntabel (Wijaya, 2021; UU Nomor 27 Tahun 2022; Alkarmi et al., 2026).

Analisis Perbandingan Pengaturan Pertanggungjawaban Korporasi di Beberapa Negara

Perkembangan regulasi perlindungan data pribadi di berbagai negara menunjukkan adanya kecenderungan global untuk memperkuat pertanggungjawaban korporasi sebagai pengendali data. Kecenderungan tersebut lahir karena korporasi digital tidak hanya berperan sebagai pelaku usaha, tetapi juga sebagai pihak yang menguasai, mengolah, menyimpan, dan memanfaatkan data pribadi masyarakat

dalam skala besar. Dalam konteks ini, data pribadi telah berubah menjadi aset ekonomi yang memiliki nilai strategis sekaligus menimbulkan risiko hukum apabila tidak dikelola secara hati-hati. Oleh karena itu, hukum modern mulai bergeser dari pendekatan yang hanya menitikberatkan pada kesalahan individu menuju pendekatan yang menilai kegagalan sistemik dalam tata kelola korporasi. Pergeseran ini penting karena kebocoran data sering kali tidak terjadi karena satu tindakan individu, melainkan akibat lemahnya sistem pengawasan, keamanan, dan kepatuhan internal perusahaan (Priyatno, 2017).

Uni Eropa melalui *General Data Protection Regulation* atau GDPR menerapkan prinsip *accountability* sebagai dasar utama dalam pengaturan perlindungan data pribadi. Prinsip ini mewajibkan setiap pengendali data untuk tidak hanya mematuhi ketentuan hukum, tetapi juga mampu membuktikan bahwa seluruh proses pengolahan data telah dilakukan sesuai standar perlindungan yang berlaku. Artinya, korporasi tidak cukup hanya menyatakan bahwa sistemnya aman, melainkan harus memiliki dokumentasi, mekanisme audit, kebijakan internal, serta prosedur teknis yang dapat menunjukkan kepatuhan tersebut. Pendekatan ini menempatkan beban tanggung jawab secara aktif pada korporasi sebagai pengendali data, bukan semata-mata pada korban atau aparat penegak hukum. Dengan demikian, GDPR memperkenalkan model pertanggungjawaban yang lebih preventif, terukur, dan berorientasi pada pembuktian kepatuhan korporasi sejak awal proses pengolahan data dilakukan (European Union, 2016).

Berbeda dengan Indonesia yang masih relatif kuat dipengaruhi paradigma pembuktian kesalahan korporasi dalam kerangka hukum pidana, GDPR menerapkan pendekatan *risk-based accountability*. Pendekatan ini menekankan bahwa semakin besar risiko pemrosesan data terhadap hak dan kebebasan subjek data, semakin besar pula kewajiban korporasi untuk menerapkan langkah perlindungan teknis dan organisatoris yang memadai. Oleh karena itu, pengenaan sanksi terhadap korporasi dalam sistem GDPR tidak selalu harus bergantung pada pembuktian adanya niat jahat secara langsung dari pengurus korporasi. Sanksi administratif yang besar dapat dikenakan apabila korporasi gagal membuktikan bahwa ia telah menerapkan standar keamanan dan kepatuhan yang layak. Model ini menunjukkan bahwa tanggung jawab korporasi dalam perlindungan data pribadi lebih tepat dipandang sebagai tanggung jawab kelembagaan yang melekat pada fungsi pengendalian data (European Union, 2016).

Di Amerika Serikat, pertanggungjawaban korporasi berkembang melalui berbagai doktrin yang lebih fleksibel dalam membaca kesalahan korporasi. Salah satu doktrin yang relevan adalah *collective knowledge doctrine*, yaitu doktrin yang memungkinkan pengetahuan beberapa individu dalam korporasi digabungkan untuk membentuk pengetahuan atau kesalahan korporasi secara keseluruhan. Melalui doktrin ini, korporasi tidak dapat berlindung di balik alasan bahwa tidak ada satu individu pun yang mengetahui seluruh unsur pelanggaran secara lengkap. Apabila beberapa bagian dalam organisasi mengetahui potongan informasi yang apabila digabungkan menunjukkan adanya risiko atau pelanggaran, maka pengetahuan tersebut dapat dianggap sebagai pengetahuan korporasi. Pendekatan ini dinilai lebih sesuai dengan karakter korporasi modern yang memiliki pembagian kerja kompleks, struktur hierarkis berlapis, serta sistem pengambilan keputusan yang tersebar (United States v. Bank of New England, 1987).

Relevansi *collective knowledge doctrine* semakin kuat apabila dikaitkan dengan platform digital yang bekerja melalui sistem algoritmik, *cloud computing*, otomatisasi data, dan jaringan pihak ketiga. Dalam praktiknya, satu unit perusahaan mungkin mengetahui adanya kelemahan sistem keamanan, unit lain mengetahui adanya peningkatan serangan siber, sementara unit manajemen mengetahui adanya keterbatasan anggaran untuk perlindungan data. Jika setiap pengetahuan tersebut dilihat secara terpisah, maka kesalahan korporasi sulit dibuktikan karena tidak ada satu individu yang menguasai keseluruhan fakta. Namun apabila seluruh pengetahuan tersebut dipandang sebagai satu kesatuan pengetahuan korporasi, maka kelalaian sistemik dapat lebih mudah diidentifikasi. Dengan demikian, doktrin ini memberikan dasar konseptual yang lebih adil untuk menilai tanggung jawab korporasi digital yang bekerja secara terdesentralisasi (Wells, 2001).

Dibandingkan dengan Uni Eropa dan Amerika Serikat, hukum Indonesia masih menghadapi tantangan dalam membangun konstruksi pertanggungjawaban korporasi yang sepenuhnya adaptif terhadap perkembangan teknologi digital. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur kewajiban pengendali data pribadi, prosesor data pribadi, sanksi administratif, serta ketentuan pidana terkait pelindungan data pribadi. Namun dalam ranah pertanggungjawaban pidana korporasi, pembuktian kesalahan masih sering menghadapi kendala karena

sistem hukum pidana Indonesia masih dipengaruhi oleh paradigma pertanggungjawaban individual. PERMA Nomor 13 Tahun 2016 memang telah memberikan pedoman penanganan perkara tindak pidana oleh korporasi, tetapi belum secara spesifik menjawab kompleksitas kesalahan korporasi dalam kasus kegagalan algoritmik dan kebocoran data digital. Kondisi ini menunjukkan perlunya pembaruan doktrin agar hukum pidana Indonesia tidak tertinggal dari perkembangan model bisnis digital (Mahkamah Agung RI, 2016).

Dalam konteks Indonesia, persoalan utama bukan hanya terletak pada ada atau tidaknya aturan mengenai korporasi sebagai subjek hukum pidana, tetapi juga pada parameter pembuktian kesalahan korporasi. Pada kasus kebocoran data, kesalahan sering kali muncul dalam bentuk pembiaran, lemahnya pengawasan, tidak adanya audit keamanan, penggunaan sistem lama, atau kegagalan memperbarui protokol keamanan siber. Bentuk kesalahan seperti ini tidak selalu mudah dibuktikan melalui konsep mens rea klasik yang mencari niat jahat dari individu tertentu. Oleh sebab itu, pendekatan yang menekankan kesalahan organisasi atau *organizational fault* menjadi lebih relevan untuk diterapkan. Melalui pendekatan tersebut, korporasi dapat dimintai pertanggungjawaban apabila terbukti gagal membangun sistem kepatuhan dan keamanan yang wajar sesuai risiko kegiatan usahanya (Widodo, 2009).

Dalam perspektif *ius constituendum*, pertanggungjawaban pidana korporasi digital di Indonesia perlu direkonstruksi melalui pengakuan terhadap konsep *corporate digital negligence*. Konsep ini dapat dipahami sebagai bentuk kelalaian korporasi yang timbul akibat kegagalan menyediakan, memelihara, dan memperbarui sistem keamanan digital yang memadai. Kelalaian tersebut dapat dinilai dari tidak adanya standar perlindungan data, lemahnya enkripsi, tidak dilakukannya audit keamanan berkala, serta tidak adanya mitigasi risiko terhadap serangan siber. Dengan pengakuan konsep ini, pembuktian kesalahan korporasi tidak lagi harus selalu dikaitkan dengan kehendak jahat direksi atau pengurus tertentu. Sebaliknya, kesalahan dapat dibuktikan melalui kegagalan korporasi dalam memenuhi kewajiban kehati-hatian digital yang seharusnya melekat pada setiap pengendali data pribadi (McPeak, 2021).

Selain itu, pemerintah perlu menetapkan standar minimum keamanan siber yang memiliki kekuatan hukum mengikat sebagai parameter objektif dalam menilai kelalaian korporasi. Standar tersebut dapat mencakup kewajiban penggunaan sistem enkripsi, manajemen akses, audit keamanan berkala, pelaporan insiden, penilaian dampak perlindungan data, serta kewajiban pembaruan sistem secara periodik. Dengan adanya standar yang jelas, aparat penegak hukum tidak hanya bergantung pada penilaian abstrak mengenai ada atau tidaknya kesalahan korporasi. Korporasi juga akan memiliki pedoman yang pasti mengenai tindakan apa saja yang wajib dilakukan untuk memenuhi prinsip kehati-hatian digital. Keberadaan standar ini penting untuk menciptakan kepastian hukum, baik bagi pelaku usaha digital maupun bagi masyarakat sebagai subjek data pribadi (Qamar dan Rezah, 2020).

Penguatan kewenangan lembaga pengawas perlindungan data pribadi juga menjadi aspek penting dalam membangun sistem pertanggungjawaban korporasi yang efektif. Lembaga pengawas perlu diberikan kewenangan untuk melakukan audit keamanan secara berkala terhadap penyelenggara sistem elektronik yang mengelola data dalam jumlah besar. Audit tersebut tidak hanya bersifat administratif, tetapi juga harus mampu menilai kualitas tata kelola risiko, kesiapan sistem keamanan, serta efektivitas mekanisme tanggap insiden. Apabila lembaga pengawas menemukan adanya kelalaian serius, hasil audit dapat digunakan sebagai dasar penegakan sanksi administratif maupun sebagai bukti awal dalam proses pidana. Dengan model ini, penegakan hukum perlindungan data tidak hanya bersifat reaktif setelah terjadi kebocoran data, tetapi juga bersifat preventif melalui pengawasan berkelanjutan (BPK RI, 2022).

Penerapan prinsip *strict liability* secara terbatas terhadap kasus kebocoran data berskala besar juga dapat dipertimbangkan dalam pembaruan hukum pidana Indonesia. Prinsip ini tidak perlu diterapkan secara luas terhadap semua pelanggaran, tetapi dapat dibatasi pada keadaan tertentu, misalnya kebocoran data yang menimbulkan kerugian besar, melibatkan data sensitif, atau terjadi akibat kegagalan korporasi memenuhi standar keamanan minimum. Penerapan terbatas tersebut bertujuan untuk mendorong korporasi agar lebih serius membangun sistem perlindungan data sejak awal. Dalam konteks platform digital, risiko yang ditimbulkan oleh kelalaian korporasi dapat berdampak luas terhadap masyarakat, sehingga dibutuhkan instrumen hukum yang memiliki efek pencegahan kuat. Oleh karena itu, *strict liability* terbatas dapat menjadi pilihan kebijakan hukum pidana yang proporsional untuk memperkuat kepatuhan korporasi digital (Muladi dan Priyatno, 2010).

Dengan demikian, perbandingan antara Uni Eropa, Amerika Serikat, dan Indonesia menunjukkan bahwa arah pembaruan hukum pidana korporasi perlu bergerak menuju pendekatan yang lebih sistemik dan adaptif. Uni Eropa memberikan pelajaran penting melalui prinsip *risk-based accountability* yang menempatkan korporasi sebagai pihak yang wajib membuktikan kepatuhan dalam pengelolaan data. Amerika Serikat memberikan contoh melalui *collective knowledge doctrine* yang memungkinkan pengetahuan terpisah dalam struktur korporasi dipandang sebagai pengetahuan kolektif perusahaan. Sementara itu, Indonesia masih perlu memperkuat konstruksi pembuktian kesalahan korporasi digital agar tidak terlalu bergantung pada kesalahan individu tertentu. Dengan model pembaruan tersebut, pertanggungjawaban pidana korporasi dapat diarahkan pada kegagalan sistemik dalam tata kelola digital, sehingga perlindungan data pribadi masyarakat menjadi lebih efektif, adil, dan sesuai dengan perkembangan teknologi informasi.

KESIMPULAN

Penelitian ini menunjukkan bahwa model pertanggungjawaban pidana korporasi yang saat ini diatur dalam UU PDP, UU ITE, dan KUHP Baru masih menghadapi berbagai hambatan implementatif ketika diterapkan terhadap platform digital modern. Hambatan tersebut terutama berkaitan dengan kesulitan pembuktian unsur kesalahan korporasi, kompleksitas hubungan kausalitas dalam sistem digital, serta belum adanya standar teknis keamanan siber yang dapat dijadikan parameter objektif untuk menilai kelalaian korporasi.

Penelitian ini juga menemukan bahwa perkembangan teknologi algoritmik dan kecerdasan buatan telah menyebabkan doktrin pertanggungjawaban pidana konvensional menjadi kurang memadai untuk menjangkau bentuk-bentuk kesalahan yang muncul dalam tata kelola platform digital. Oleh karena itu, diperlukan rekonstruksi konsep pertanggungjawaban pidana korporasi melalui pendekatan aggregation theory, collective corporate knowledge, dan corporate digital negligence agar sistem hukum pidana Indonesia mampu memberikan perlindungan yang lebih efektif terhadap data pribadi masyarakat. Dari sisi kebijakan hukum, pembentukan standar keamanan siber nasional yang mengikat, penguatan kewenangan lembaga pengawas data pribadi, serta pengembangan mekanisme audit keamanan digital menjadi langkah strategis yang perlu dilakukan guna mewujudkan sistem perlindungan data pribadi yang lebih efektif dan berkeadilan.

REFERENSI

Akila, N., & Lukitasari, D. (2024). Tindak pidana pencurian data dan privasi pengguna dalam transaksi e-commerce: Studi kasus pada aplikasi Tokopedia. Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, 1(2), 115–126. https://doi.org/10.62383/amandemen.v1i2.145

Arief, L. S., & Purwanto, R. (2025). Tinjauan yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam menangani kebocoran data pelanggan e-commerce. Pemuliaan Keadilan, 2(3), 85–102. https://doi.org/10.62383/pk.v2i3.1019

Chika, G., Putra, F. P., & Firdaus, Z. (2025). Analisis yuridis kebocoran data pribadi dalam perspektif hukum siber Indonesia. Jurnal Hukum Nasional.

Chushairi, S. M., Fithry, A., & Rusfandi, R. (2025). Perlindungan hukum bagi korban atas kebocoran Pusat Data Nasional Sementara (PDNs) perspektif perlindungan data pribadi. Jurnal Jendela Hukum, 12(2), 89–122. https://doi.org/10.24929/jjh.v12i2.4664

Dachlan, A. A., Nabila, A., Putri, N. A., & Nurmasitha, N. (2025). Pertanggungjawaban hukum pemerintah dalam kebocoran data pribadi pada penyelenggaraan Pusat Data Nasional. Jurnal Hukum Samudra Keadilan, 20(1), 109–124. https://doi.org/10.33059/jhsk.v20i1.11279

Fritiana, A., Daishahwa, & Wiraguna, S. A. (2025). Penyalahgunaan data pribadi pada layanan pinjaman online: Analisis perlindungan dan sanksi hukum. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3(2), 523–529. https://doi.org/10.61104/alz.v3i2.1082

Husri, H., & Samsul. (2026). Pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik dalam perspektif UU Perlindungan Data Pribadi. Progresif: Jurnal Hukum, 20(1), 183–204. https://doi.org/10.33019/fk5vwp69

Ismaidar, I., & Ula, R. F. (2025). Pertanggungjawaban pidana korporasi terhadap kebocoran data pribadi konsumen dalam perspektif hukum pidana siber di Indonesia. Hukum Inovatif, 2(3), 44–51.

Kristanto, A. R., & Slamet, S. R. (2026). Legal liability of financial services institutions for personal data leakage under the Personal Data Protection Act. Golden Ratio of Data in Summary, 6(1), 83–90. https://doi.org/10.52970/grdis.v6i1.1981

Mangkunegara, R. M. A. (2025). Corporate criminal liability for cybersecurity: Rechtsvinding in adopting the concept of corporate manslaughter in Indonesia. Jurnal RechtsVinding: Media Pembinaan Hukum Nasional, 14(2). http://dx.doi.org/10.33331/rechtsvinding.v14i2.2193

Marzuki, P. M. (2017). Penelitian hukum. Prenada Media.

Muhni, A., Basri, M., Rivanie, S. S., Muthia, N. F., & Amri, U. (2026). From contractual breach to corporate criminal liability: Exploitation of debtor data by account officers in Indonesia. Justisi, 12(2), 513–530. https://doi.org/10.33506/js.v12i2.5298

Peran hukum pidana dalam perlindungan data pribadi dan penanggulangan cyber crime di Indonesia. (2025). Aliansi: Jurnal Hukum dan Kebijakan Digital.

Priyatno, D. (2017). Sistem pertanggungjawaban pidana korporasi dalam kebijakan legislasi. Prenada Media.

Qamar, N., & Rezah, F. S. (2020). Metode penelitian hukum: Doktrinal dan non-doktrinal. Social Politic Genius.

Samad, R. P., Ardiansyah, A., & Nabilah, E. A. (2025). A critical analysis of corporate criminal liability in Law Number 1 of 2023. SIGn Jurnal Hukum, 7(2), 664–681. https://doi.org/10.37276/sjh.v7i2.515

Simanjuntak, S. Y., & Waluyo, B. (2025). Criminal liability for hacking personal data through ransomware attacks on digital service providers in Indonesia. Jurnal Daulat Hukum, 8(4), 851. https://doi.org/10.30659/jdh.v8i4.48885

Simanullang, B. R. H. (2026). Piercing the corporate veil: The urgency of criminal liability of directors in personal data protection law. Nalarnagara Journal.

Wasahua, I., & Awalia, R. P. (2025). Pertanggungjawaban hukum terhadap pelaku penyalahgunaan data pribadi: Studi Putusan Pengadilan Negeri Tangerang No. 76/Pid.Sus/2024/PN Tng. Rewang Rencang: Jurnal Hukum Lex Generalis, 6(12).

Watkat, F. X., Ingratubun, M. T., Ingsaputro, M. H., & Hartantyo, A. T. (2024). Pertanggungjawaban pidana pengendali data pribadi terhadap kebocoran data pribadi warga negara Indonesia. Jurnal Hukum Ius Publicum, 5(2), 177–198. https://doi.org/10.55551/jip.v5i2.175 Widodo. (2009). Sistem pemidanaan dalam cybercrime. Laksbang Mediatama.