JIM: Jurnal Ilmu Multidisiplin
E-ISSN : 2829-4580
P-ISSN : 2829-4599
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/jim.v4i5

Aspek Hukum Keamanan Siber dalam Penggunaan AI dan Big Data oleh Inovasi Teknologi Sektor Keuangan (ITSK)

Arnold Rezon[1]
[1]Universitas Pelita Harapan, Surabaya, Indonesia, Arnoldrezon@gmail.com

Corresponding Author: Arnoldrezon@gmail.com[1]

Abstract: *The digital transformation of the financial sector has given rise to Financial Sector Technology Innovation (ITSK), which utilizes Artificial Intelligence (AI) and big data to create faster, more efficient, and inclusive financial services. However, this technological advancement also introduces new legal challenges related to cybersecurity and personal data protection. This study aims to analyze the legal aspects of cybersecurity in the use of AI and big data by ITSK, as well as the legal liability of ITSK operators in cases of data breaches. This research employs a normative juridical method with statutory, conceptual, and case approaches, using primary, secondary, and tertiary legal materials. The findings indicate that Indonesia does not yet have a single comprehensive regulation governing cybersecurity in AI and big data; however, sectoral regulations such as the Personal Data Protection Act (PDP Law), the Electronic Information and Transactions Act (ITE Law), OJK Regulations, and BSSN guidelines serve as the foundational legal framework. The strict liability principle places absolute responsibility on ITSK operators as data controllers, while the technoethics theory emphasizes moral obligations to ensure technology is used fairly and transparently. The study concludes that effective legal protection against data breaches in the ITSK ecosystem requires strengthening technical regulations, enhancing coordination among regulatory authorities, and integrating responsive legal and ethical principles in digital governance.*

Keywords: *cybersecurity, Artificial Intelligence, big data, ITSK, personal data protection.*

Abstrak: Transformasi digital di sektor keuangan telah melahirkan Inovasi Teknologi Sektor Keuangan (ITSK) yang memanfaatkan Artificial Intelligence (AI) dan big data untuk menciptakan layanan yang cepat, efisien, dan inklusif. Namun, pemanfaatan teknologi ini memunculkan tantangan hukum baru terkait keamanan siber dan perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis aspek hukum keamanan siber dalam penggunaan AI dan big data oleh ITSK serta bentuk pertanggungjawaban hukum pengelolanya terhadap kebocoran data konsumen. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, menggunakan bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa Indonesia belum memiliki regulasi tunggal yang secara komprehensif mengatur keamanan siber AI dan big data, namun terdapat berbagai peraturan sektoral seperti UU PDP, UU ITE, POJK, dan regulasi BSSN yang menjadi landasan perlindungan hukum. Prinsip strict liability menempatkan tanggung jawab mutlak pada penyelenggara ITSK sebagai pengendali data pribadi, sedangkan teori

technoethics menekankan kewajiban moral atas penggunaan teknologi secara adil dan transparan. Penelitian ini menyimpulkan bahwa efektivitas perlindungan hukum terhadap kebocoran data dalam ekosistem ITSK membutuhkan penguatan regulasi teknis, koordinasi antar-lembaga pengawas, serta penerapan prinsip hukum dan etika digital yang responsif terhadap perkembangan teknologi.

Kata Kunci: leamanan siber, Artificial Intelligence, big data, ITSK, perlindungan data pribadi.

PENDAHULUAN

Transformasi digital telah menjadi pendorong utama dalam perubahan sistem keuangan global. Di Indonesia, kemajuan teknologi informasi mendorong munculnya Inovasi Teknologi Sektor Keuangan (ITSK), yaitu pemanfaatan teknologi mutakhir seperti Artificial Intelligence (AI) dan *big data analytics* untuk menciptakan layanan keuangan yang lebih cepat, efisien, dan inklusif. Melalui ITSK, berbagai layanan seperti *fintech lending*, *digital banking*, *robo-advisory*, dan sistem *credit scoring* berbasis algoritma berkembang pesat untuk menjangkau masyarakat yang sebelumnya belum terlayani oleh sistem keuangan konvensional (Ozili, 2021).

Namun, di balik manfaat tersebut, pemanfaatan teknologi ini juga menimbulkan tantangan hukum dan etika yang kompleks, terutama dalam aspek keamanan siber dan perlindungan data pribadi. Data nasabah yang dikumpulkan, dianalisis, dan disimpan oleh sistem berbasis AI dan *big data* bersifat sangat sensitif karena mencakup informasi identitas, transaksi keuangan, perilaku digital, hingga informasi biometrik (Galla, 2020) . Jika data tersebut disalahgunakan atau bocor, dampaknya dapat merugikan konsumen, merusak reputasi penyelenggara layanan keuangan, dan mengganggu stabilitas sistem keuangan digital secara keseluruhan.

Fenomena kebocoran data, seperti yang terjadi pada kasus Tokopedia dan sejumlah aplikasi *pinjaman online*, menjadi bukti nyata lemahnya tata kelola keamanan siber di sektor keuangan digital (Barratut Taqiyyah Rafie, 2021) . Akses ilegal terhadap data pribadi, penyebaran informasi tanpa izin, dan praktik penagihan yang melanggar privasi menunjukkan bahwa perlindungan hukum terhadap data pribadi masih belum optimal(Tim Detikcom, 2022). Kondisi ini mengindikasikan bahwa perkembangan teknologi belum sepenuhnya diimbangi oleh kesiapan sistem hukum dalam mengatur risiko digital yang muncul.

Pemerintah Indonesia telah berupaya membangun kerangka hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Otoritas Jasa Keuangan (OJK) dan Badan Siber dan Sandi Negara (BSSN) yang mengatur tata kelola keamanan informasi (Ifdal Lilahi et al., 2025) . Meskipun demikian, peraturan yang ada masih bersifat sektoral dan belum secara komprehensif mengatur penggunaan AI dan *big data* dalam konteks keamanan siber sektor keuangan.

Kelemahan koordinasi antarotoritas, ketiadaan standar akuntabilitas teknologi, serta rendahnya kesadaran pelaku usaha terhadap etika digital semakin memperbesar risiko pelanggaran hak privasi konsumen. Dalam konteks ini, teori Perlindungan Hukum sebagaimana dikemukakan oleh Philipus M. Hadjon menjadi relevan untuk menilai sejauh mana negara mampu memberikan perlindungan hukum yang efektif, baik secara preventif maupun represif (Hadjon, 1987) . Di sisi lain, teori *strict liability* menegaskan bahwa pengendali data—dalam hal ini pengelola ITSK—harus bertanggung jawab penuh atas setiap pelanggaran keamanan data yang terjadi, tanpa perlu dibuktikan unsur kesalahan (Aghia Khumaesi Suud, 2023).

Selain itu, teori *technoethics* memberikan perspektif moral bahwa teknologi tidak dapat dilepaskan dari nilai-nilai kemanusiaan, keadilan, dan transparansi(Mario Bunge, 1977). Oleh karena itu, penyelenggara ITSK tidak hanya berkewajiban mematuhi hukum positif, tetapi juga harus memastikan bahwa penggunaan AI dan *big data* dilakukan secara etis dan tidak merugikan hak digital konsumen.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan untuk menjawab dua permasalahan utama: (1) bagaimana aspek hukum yang mengatur keamanan siber dalam penggunaan teknologi AI dan *big data* oleh ITSK di Indonesia; dan (2) bagaimana bentuk pertanggungjawaban hukum pengelola ITSK terhadap kebocoran data konsumen. Penelitian ini bertujuan untuk menganalisis kecukupan regulasi yang ada serta memberikan rekomendasi terhadap penguatan sistem hukum yang mampu menjamin keamanan siber dan perlindungan data pribadi secara efektif di era digital.

METODE

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu penelitian hukum yang berfokus pada pengkajian terhadap norma-norma hukum positif serta teori-teori hukum yang relevan dengan isu keamanan siber dan perlindungan data pribadi dalam penggunaan Artificial Intelligence (AI) dan *big data* oleh Inovasi Teknologi Sektor Keuangan (ITSK). Penelitian yuridis normatif dipilih karena permasalahan yang dikaji bersifat konseptual dan berkaitan langsung dengan kecukupan serta penerapan regulasi yang berlaku.

Pendekatan yang digunakan dalam penelitian ini meliputi tiga pendekatan utama, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menganalisis berbagai ketentuan hukum yang berkaitan dengan perlindungan data dan keamanan siber, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta Peraturan Otoritas Jasa Keuangan (POJK), Peraturan Bank Indonesia (PBI), dan regulasi dari Badan Siber dan Sandi Negara (BSSN). Pendekatan konseptual digunakan untuk menelaah teori-teori hukum yang relevan, seperti Teori Perlindungan Hukum oleh Philipus M. Hadjon, Teori *Strict Liability*, dan Teori *Technoethics*, yang menjadi dasar analisis terhadap tanggung jawab hukum pengelola ITSK. Sedangkan pendekatan kasus digunakan untuk menelusuri insiden kebocoran data di sektor keuangan digital, seperti kasus kebocoran data Tokopedia dan pelanggaran privasi oleh sejumlah aplikasi *fintech lending* di Indonesia.

Jenis bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan perundang-undangan, kebijakan lembaga pemerintah, serta dokumen resmi dari OJK, BI, dan BSSN. Bahan hukum sekunder meliputi buku, jurnal ilmiah, artikel, dan hasil penelitian terdahulu yang membahas tentang keamanan siber, AI, *big data*, serta perlindungan hukum terhadap konsumen digital. Sedangkan bahan hukum tersier digunakan sebagai pendukung, seperti kamus hukum, ensiklopedia, dan sumber referensi tambahan yang membantu memperjelas terminologi hukum dan teknologi.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri sumber-sumber hukum yang relevan baik dari media cetak maupun daring. Analisis data dilakukan secara kualitatif dengan cara menafsirkan norma hukum yang berlaku dan mengaitkannya dengan teori-teori hukum serta fakta empiris dalam kasus-kasus kebocoran data yang terjadi. Dari hasil analisis tersebut, penulis menarik kesimpulan mengenai efektivitas perlindungan hukum terhadap keamanan siber dalam penggunaan AI dan *big data* oleh ITSK, serta merumuskan rekomendasi kebijakan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi keuangan digital.

HASIL DAN PEMBAHASAN

Aspek Hukum Keamanan Siber dalam Penggunaan Teknologi Artificial Intelligence dan Big Data oleh Inovasi Teknologi Sektor Keuangan (ITSK)

Perkembangan teknologi digital dalam sektor keuangan melalui Inovasi Teknologi Sektor Keuangan (ITSK) telah mengubah wajah sistem keuangan nasional menjadi lebih efisien, transparan, dan berbasis data. Pemanfaatan Artificial Intelligence (AI) dan *big data analytics* dalam layanan seperti *digital banking*, *fintech lending*, *robo-advisory*, dan sistem pembayaran elektronik membawa dampak signifikan terhadap kemudahan akses serta personalisasi layanan bagi konsumen. Namun, di balik kemajuan tersebut, muncul ancaman baru terhadap keamanan siber dan perlindungan data pribadi yang menjadi tantangan besar bagi sistem hukum di Indonesia.

Keamanan siber dalam konteks ITSK tidak hanya berkaitan dengan perlindungan sistem elektronik dari serangan atau akses ilegal, tetapi juga mencakup jaminan atas hak privasi dan kendali konsumen terhadap data pribadinya. Penggunaan AI dan *big data* memungkinkan pengumpulan dan analisis data dalam skala besar, termasuk data sensitif seperti identitas, transaksi keuangan, lokasi, hingga perilaku digital pengguna(Scott Robinson & Alexander S. Gillis, 2023). Tanpa sistem keamanan yang memadai, data tersebut berisiko mengalami penyalahgunaan, kebocoran, atau eksploitasi oleh pihak yang tidak berwenang.

Dari sisi hukum positif, Indonesia telah memiliki sejumlah regulasi yang mengatur keamanan siber dan perlindungan data dalam konteks digital, meskipun belum ada satu payung hukum yang secara komprehensif mengatur penggunaan AI dan *big data* dalam sektor keuangan. Regulasi utama yang relevan antara lain sebagai berikut:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP menjadi dasar hukum utama dalam pengelolaan data pribadi di Indonesia. Pasal 35 sampai dengan Pasal 37 mewajibkan pengendali data untuk menerapkan standar keamanan yang ketat, mencegah kebocoran, serta memastikan integritas sistem informasi. Pasal 41 mengatur kewajiban pelaporan insiden kebocoran data kepada otoritas dan subjek data, sedangkan Pasal 58 menetapkan tanggung jawab pengendali data atas kerugian yang timbul akibat pelanggaran. Regulasi ini mempertegas tanggung jawab hukum penyelenggara ITSK sebagai *data controller* yang wajib menjamin keamanan dan kerahasiaan data konsumen.
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan melalui UU Nomor 19 Tahun 2016. UU ITE memberikan dasar hukum bagi pelaksanaan sistem elektronik dan transaksi digital, termasuk kewajiban penyelenggara sistem untuk menjaga keandalan dan keamanan sistemnya sebagaimana diatur dalam Pasal 15. Pasal 30 hingga Pasal 32 melarang akses ilegal, peretasan, serta penyebaran data tanpa izin. UU ITE menjadi landasan hukum umum yang memperkuat aspek keamanan teknologi informasi dalam operasional ITSK.
3. Peraturan Otoritas Jasa Keuangan (OJK) Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital (IKD).
   POJK ini secara khusus mengatur penyelenggara ITSK, termasuk kewajiban menjaga kerahasiaan dan keamanan data pengguna (Pasal 23) serta melakukan *regulatory sandbox* sebelum memperoleh izin operasional penuh (Pasal 27). Pendekatan ini mencerminkan bentuk perlindungan hukum preventif, di mana setiap inovasi digital diuji terlebih dahulu dari sisi keamanan dan kepatuhan hukum sebelum diterapkan secara luas.
4. Peraturan Bank Indonesia (BI) dan Regulasi Badan Siber dan Sandi Negara (BSSN). BI melalui PBI Nomor 22/23/PBI/2020 tentang Sistem Pembayaran dan PBI Nomor 23/6/PBI/2021 tentang Perlindungan Konsumen mempertegas kewajiban penyelenggara sistem pembayaran untuk menerapkan *business continuity plan*, audit

keamanan, serta jaminan perlindungan data pengguna. Sementara itu, BSSN menerbitkan Peraturan Nomor 4 Tahun 2021 tentang Manajemen Risiko Siber dan mendorong penerapan standar internasional ISO/IEC 27001 dalam sistem manajemen keamanan informasi.

Meskipun telah terdapat berbagai instrumen hukum tersebut, kerangka regulasi Indonesia masih bersifat sektoral dan terfragmentasi. Tidak ada satu peraturan yang secara eksplisit mengatur tata kelola AI dan *big data* dalam sistem keuangan digital secara komprehensif. Hal ini menimbulkan celah hukum dalam aspek transparansi algoritma, tanggung jawab atas keputusan otomatis (*automated decision-making*), serta audit etis terhadap sistem AI yang digunakan untuk pengambilan keputusan keuangan.

Jika dianalisis menggunakan Teori Perlindungan Hukum dari Philipus M. Hadjon, sistem hukum Indonesia telah mengarah pada dua bentuk perlindungan, yaitu preventif dan represif. Perlindungan preventif diwujudkan melalui regulasi yang mewajibkan standar keamanan data, audit sistem, dan mekanisme pengawasan teknologi. Sedangkan perlindungan represif diwujudkan melalui sanksi administratif, pidana, maupun perdata terhadap pelaku usaha atau pengendali data yang melanggar kewajiban hukum. Namun, dalam praktiknya, bentuk perlindungan ini belum efektif karena lemahnya penegakan hukum, keterbatasan kapasitas teknis aparat, dan kurangnya koordinasi antarotoritas.

Selain itu, penerapan Teori Strict Liability menjadi penting untuk memberikan kepastian hukum bagi konsumen. Berdasarkan prinsip ini, pengendali data dapat dimintai pertanggungjawaban secara mutlak atas terjadinya kebocoran data, meskipun tanpa pembuktian unsur kesalahan. Pendekatan ini relevan dalam konteks digital, di mana kompleksitas sistem AI dan *big data* sering kali membuat pembuktian kesalahan teknis hampir mustahil dilakukan oleh korban atau konsumen.

Dari perspektif Technoethics, keamanan siber tidak hanya menjadi isu hukum dan teknis, tetapi juga moral dan sosial. Penggunaan AI dan *big data* oleh ITSK harus tunduk pada prinsip etika digital: keadilan, transparansi, non-diskriminasi, dan akuntabilitas algoritmik. Misalnya, sistem *credit scoring* berbasis AI tidak boleh menimbulkan bias terhadap kelompok tertentu atau mengambil keputusan otomatis tanpa mekanisme *human oversight*. Oleh karena itu, penyelenggara ITSK memiliki kewajiban moral untuk memastikan bahwa setiap inovasi teknologi tetap berada dalam koridor kemanusiaan dan keadilan sosial.

Dengan demikian, dapat disimpulkan bahwa meskipun Indonesia telah memiliki dasar hukum untuk menjamin keamanan siber dalam penggunaan AI dan *big data* oleh ITSK, kerangka regulasi yang ada masih memerlukan harmonisasi, integrasi, dan penguatan pada aspek akuntabilitas serta etika teknologi. Dibutuhkan mekanisme hukum yang lebih adaptif terhadap kemajuan teknologi, peningkatan kapasitas penegak hukum, dan kolaborasi lintas lembaga agar keamanan siber tidak hanya menjadi kewajiban administratif, tetapi juga wujud nyata perlindungan hak digital konsumen dalam ekosistem keuangan modern.

Pertanggungjawaban Hukum Pengelola Inovasi Teknologi Sektor Keuangan (ITSK) terhadap Kebocoran Data Konsumen

Perkembangan Inovasi Teknologi Sektor Keuangan (ITSK) yang memanfaatkan Artificial Intelligence (AI) dan *big data* membawa tantangan besar terhadap perlindungan hukum atas data pribadi konsumen. Dalam sistem hukum Indonesia, penyelenggara ITSK memiliki kedudukan sebagai *pengendali data pribadi* (*data controller*) sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Posisi ini menegaskan bahwa mereka bertanggung jawab penuh terhadap seluruh siklus pemrosesan data pribadi, mulai dari pengumpulan, penyimpanan, pengolahan, hingga penghapusan data.

Sebagai pengendali data, penyelenggara ITSK tidak hanya memiliki tanggung jawab teknis, tetapi juga tanggung jawab hukum dan etis atas keamanan data yang mereka kelola.

Dalam konteks hukum positif, pertanggungjawaban hukum terhadap kebocoran data dapat dibagi menjadi tiga bentuk utama, yaitu pertanggungjawaban perdata, pidana, dan administratif.

Pertama, pertanggungjawaban perdata muncul ketika penyelenggara ITSK gagal memenuhi kewajiban hukum dalam menjaga keamanan data pengguna. Berdasarkan Pasal 58 UU PDP dan Pasal 1365 KUHPerdata, pengendali data wajib mengganti kerugian yang dialami oleh subjek data akibat pemrosesan data yang melanggar hukum. Dalam konteks ini, asas *strict liability* diterapkan, yaitu tanggung jawab hukum melekat tanpa memerlukan pembuktian unsur kesalahan. Prinsip ini penting mengingat korban kebocoran data sering kali tidak memiliki kemampuan teknis untuk membuktikan penyebab kebocoran atau kelalaian sistem secara langsung.

Kedua, pertanggungjawaban pidana diberlakukan apabila kebocoran data disertai dengan unsur kesengajaan, kelalaian berat, atau penyalahgunaan data pribadi. Pasal 67 sampai dengan Pasal 70 UU PDP menetapkan sanksi pidana bagi setiap pihak yang dengan sengaja mengungkapkan atau menggunakan data pribadi tanpa hak. Selain itu, Pasal 30 hingga Pasal 32 UU ITE juga mengatur pidana atas akses ilegal dan peretasan sistem elektronik. Dalam konteks ini, tanggung jawab dapat dikenakan baik kepada badan hukum penyelenggara ITSK maupun individu di dalamnya, seperti direksi atau pengelola sistem, apabila terbukti berperan langsung dalam pelanggaran.

Ketiga, pertanggungjawaban administratif diterapkan oleh lembaga pengawas seperti OJK, Kominfo, dan otoritas PDP. Sanksi administratif yang dapat dijatuhkan meliputi teguran tertulis, denda administratif, pembekuan sementara kegiatan usaha, hingga pencabutan izin operasional. Berdasarkan POJK Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital dan UU PDP, penyelenggara ITSK juga diwajibkan untuk melaporkan insiden kebocoran data dalam jangka waktu tertentu sebagai bagian dari mekanisme akuntabilitas publik.

Dalam perspektif Teori Perlindungan Hukum oleh Philipus M. Hadjon, tanggung jawab hukum pengelola ITSK merupakan bentuk perlindungan hukum represif yang diberikan negara kepada konsumen. Perlindungan ini baru berjalan efektif jika korban kebocoran data memperoleh akses terhadap pemulihan hak, baik dalam bentuk ganti rugi maupun rehabilitasi data. Namun, pada praktiknya, sebagian besar kasus kebocoran data di Indonesia berakhir tanpa proses hukum yang jelas atau pemulihan konkret bagi korban, yang menunjukkan lemahnya pelaksanaan prinsip keadilan substantif dalam hukum perlindungan data.

Penerapan Teori Strict Liability semakin mempertegas bahwa pengelola ITSK wajib bertanggung jawab penuh atas insiden kebocoran data, meskipun tanpa pembuktian unsur kesalahan. Dalam konteks AI dan *big data*, teori ini menjadi relevan karena kompleksitas teknologi sering kali membuat penyebab kebocoran sulit diidentifikasi. Dengan prinsip ini, setiap pengendali data diwajibkan melakukan langkah preventif maksimal, seperti enkripsi data, audit sistem, dan evaluasi risiko keamanan secara berkala.

Selain tanggung jawab hukum formal, penyelenggara ITSK juga memiliki kewajiban moral yang bersumber dari Teori Technoethics. Dalam era digital, tanggung jawab tidak berhenti pada kepatuhan hukum, tetapi juga mencakup kewajiban etis untuk memastikan bahwa teknologi yang digunakan tidak menimbulkan kerugian sosial, diskriminasi algoritmik, atau pelanggaran terhadap hak-hak digital konsumen. Penggunaan AI dalam *credit scoring* misalnya, harus dilakukan secara transparan dan dapat dipertanggungjawabkan agar tidak menciptakan bias terhadap kelompok tertentu. Dengan demikian, technoethics berfungsi sebagai pedoman moral bagi pengelola ITSK agar keamanan siber tidak hanya dilihat dari sisi teknis, tetapi juga sebagai bagian dari keadilan sosial digital.

Untuk memperkuat efektivitas pertanggungjawaban hukum pengelola ITSK, dibutuhkan beberapa langkah strategis. Pertama, penyusunan standar audit algoritma dan mekanisme *explainability* terhadap keputusan otomatis agar prinsip akuntabilitas dapat

diterapkan secara konkret. Kedua, pembentukan sistem koordinasi lintas lembaga antara OJK, BI, Kominfo, dan BSSN dalam menangani insiden kebocoran data agar tidak terjadi tumpang tindih kewenangan. Ketiga, penguatan mekanisme pemulihan hak konsumen melalui jalur administratif dan *class action* untuk memberikan keadilan substantif bagi korban kebocoran data.

Dengan demikian, tanggung jawab hukum pengelola ITSK terhadap kebocoran data tidak hanya berlandaskan pada kepatuhan formal terhadap regulasi, tetapi juga harus berorientasi pada prinsip keadilan, transparansi, dan tanggung jawab sosial. Pendekatan yang menggabungkan asas hukum positif, prinsip *strict liability*, serta nilai-nilai technoethics merupakan kunci dalam membangun tata kelola digital yang aman, etis, dan berkeadilan bagi seluruh pemangku kepentingan di sektor keuangan.

KESIMPULAN

Pemanfaatan Artificial Intelligence (AI) dan *big data* dalam Inovasi Teknologi Sektor Keuangan (ITSK) telah membawa perubahan signifikan terhadap sistem keuangan Indonesia. Teknologi ini berperan penting dalam meningkatkan efisiensi, inklusivitas, dan personalisasi layanan keuangan, sekaligus memperkuat daya saing industri di era digital. Namun, kemajuan tersebut juga diiringi oleh meningkatnya risiko hukum dan etika, terutama dalam hal keamanan siber dan perlindungan data pribadi. Ketika data nasabah dikumpulkan dan dianalisis secara masif oleh sistem berbasis AI, potensi kebocoran, penyalahgunaan, serta diskriminasi algoritmik menjadi isu yang tak terhindarkan.

Hasil penelitian menunjukkan bahwa aspek hukum yang mengatur keamanan siber dan perlindungan data dalam penggunaan AI dan *big data* oleh ITSK di Indonesia masih bersifat sektoral dan belum terintegrasi. Regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Otoritas Jasa Keuangan (OJK), Peraturan Bank Indonesia (BI), dan regulasi Badan Siber dan Sandi Negara (BSSN) telah memberikan landasan hukum awal, tetapi belum cukup menjawab kompleksitas teknologi keuangan modern. Ketiadaan aturan teknis terkait transparansi algoritma, tanggung jawab otomatisasi keputusan, serta audit etis terhadap sistem AI menunjukkan masih adanya celah dalam sistem hukum nasional.

Bentuk pertanggungjawaban hukum pengelola ITSK terhadap kebocoran data dapat ditinjau dari tiga aspek: perdata, pidana, dan administratif. Prinsip *strict liability* sebagaimana tercantum dalam UU PDP menegaskan bahwa pengendali data tetap bertanggung jawab penuh atas kerugian akibat kebocoran data, meskipun tanpa pembuktian unsur kesalahan. Pendekatan ini dianggap paling relevan untuk menjamin kepastian hukum dan perlindungan konsumen di tengah kompleksitas teknologi digital. Selain itu, teori *technoethics* menegaskan bahwa tanggung jawab hukum tidak hanya bersifat normatif, tetapi juga etis. Penyelenggara ITSK harus memastikan bahwa teknologi yang mereka operasikan tidak mencederai nilai keadilan, transparansi, dan hak asasi digital pengguna.

Penelitian ini menyimpulkan bahwa perlindungan hukum terhadap keamanan siber dalam ekosistem ITSK di Indonesia belum berjalan optimal. Diperlukan pembaruan hukum yang lebih komprehensif melalui integrasi lintas sektor, peningkatan kapasitas lembaga pengawas, serta penyusunan standar akuntabilitas teknologi seperti audit algoritma dan *explainability framework*. Pemerintah dan lembaga regulator perlu memperkuat koordinasi dalam pengawasan, sementara pelaku usaha ITSK harus menanamkan prinsip *compliance by design* dan *ethics by default* dalam setiap inovasi teknologi yang dikembangkan. Dengan demikian, pengelolaan AI dan *big data* di sektor keuangan dapat berjalan seimbang antara efisiensi teknologi dan perlindungan hak-hak digital masyarakat.

REFERENSI

Barratut Taqiyyah Rafie. (2021, September 3). Begini cara cek aplikasi pinjol yang bisa intip nomor kontak teman di ponsel. *Kompas*.

Galla, E. P. (2020). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions. *Educational Administration: Theory and Practice*, 1228–1236. https://doi.org/10.53555/kuey.v27i4.7592

Hadjon, P. M. (1987). *Perlindungan Hukum bagi Rakyat di Indonesia: Sebuah Studi tentang Prinsip-prinsipnya dalam Hukum Tata Negara*. Bina Ilmu.

Ifdal Lilahi, Lis Febrianda, & Desmal Fajri. (2025). KEPASTIAN HUKUM DALAM PELINDUNGAN DATA PRIBADI BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI. *Universitas Bung Hatta*. http://repo.bunghatta.ac.id/id/eprint/25189

Aghia Khumaesi Suud. (2023). *ANALISIS PENERAPAN KONSEP PERTANGGUNGJAWABAN MUTLAK (STRICT LIABILITY) DALAM KASUS KORUPSI* (Vol. 52, Issue 2).

Mario Bunge. (1977). *TOWARDS A TECHNOETHICS* (Vol. 60). JSTOR.

Ozili, P. K. (2021). *Big data and artificial intelligence for financial inclusion: benefits and issues*. https://doi.org/10.2139/ssrn.3766097

Scott Robinson, & Alexander S. Gillis. (2023). *5V's of big data*. Tech Target. https://www.techtarget.com/searchdatamanagement/definition/5-Vs-of-big-data

Tim Detikcom. (2022, January 18). Pinjol Ilegal WA Blast Ancaman ke Seluruh Kontak HP, Saya Harus Lapor Siapa? *Detik.Com*.