Tanggung Jawab Hukum Direksi atas Keamanan Siber dalam Tata Kelola Perusahaan Digital

Burhanudin[1]
[1]**Fakultas Hukum Universitas Nahdlatul Ulama Nusa Tenggara Barat, Indonesia**
Email : burhanudin@ununtb.ac.id [1]

Abstrak

Penelitian ini bertujuan untuk menganalisis pengaturan tanggung jawab direksi atas keamanan siber dalam tata kelola perusahaan digital menurut hukum Indonesia serta merumuskan konstruksi hukum yang mampu memberikan kepastian hukum terhadap tanggung jawab tersebut. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum terdiri atas bahan hukum primer, sekunder, dan tersier yang dikumpulkan melalui studi kepustakaan serta dianalisis menggunakan penafsiran hukum, teori hukum, dan asas hukum yang relevan. Hasil penelitian menunjukkan bahwa tanggung jawab direksi atas keamanan siber merupakan bagian dari fungsi pengurusan perseroan karena berkaitan dengan pengelolaan risiko digital, keandalan sistem elektronik, dan perlindungan data. Konstruksi hukum tanggung jawab direksi perlu menempatkan keamanan siber sebagai bagian dari kebijakan strategis perusahaan melalui penguatan tata kelola, pengawasan, dan pengendalian risiko. Penguatan standar kewajiban direksi diperlukan untuk mewujudkan keseimbangan antara perlindungan kepentingan perseroan dan kepastian hukum dalam penyelenggaraan perusahaan digital serta memberikan perlindungan terhadap para pihak yang berkepentingan dalam ekosistem bisnis berbasis teknologi informasi yang terus berkembang.

Kata Kunci: keamanan siber; direksi; perusahaan digital; tata kelola perusahaan; tanggung jawab hukum

Abstract

This study aims to analyze the regulation of the board of directors' liability regarding cybersecurity within digital corporate governance under Indonesian law and to formulate a legal framework that provides legal certainty regarding such liability. The study employs a normative legal research method, utilizing both statutory and conceptual approaches. Legal materials comprising primary, secondary, and tertiary sources were gathered through literature review and analyzed using relevant legal interpretation, legal theory, and legal principles. The findings indicate that the board of directors' liability for cybersecurity constitutes part of the company's management function, as it relates to digital risk management, the reliability of electronic systems, and data protection. The legal framework for directors' liability must position cybersecurity as an integral part of corporate strategic policy by strengthening governance, oversight, and risk control. Strengthening the standards of directors' obligations is essential to strike a balance between protecting the company's interests and ensuring legal certainty in digital business operations, while also safeguarding stakeholders within the rapidly evolving information technology-based business ecosystem.

Keywords**:** cybersecurity; board of directors; digital company; corporate governance; legal liability.

Retorika : Journal of Law, Social, and Humanities is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi tata kelola perusahaan menuju sistem yang semakin terdigitalisasi. Pemanfaatan komputasi awan (*cloud computing*), kecerdasan artifisial (*artificial intelligence*), *big data*, serta berbagai platform digital telah meningkatkan efektivitas dan efisiensi kegiatan usaha. Di sisi lain, transformasi tersebut juga meningkatkan risiko keamanan siber berupa serangan siber, kebocoran data, *ransomware*, pencurian informasi perusahaan, hingga gangguan terhadap sistem elektronik yang dapat menghambat keberlangsungan usaha.[1] Risiko tersebut tidak lagi dipandang sebagai persoalan teknis semata, melainkan telah berkembang menjadi bagian dari tata kelola perusahaan yang memerlukan perhatian serius dari organ perseroan, khususnya direksi sebagai pihak yang bertanggung jawab atas pengurusan perusahaan.

Dalam perspektif hukum perusahaan, direksi bertanggung jawab mengurus perseroan dengan itikad baik, penuh tanggung jawab, dan kehati-hatian. Dalam perusahaan digital, tanggung jawab tersebut mencakup pengelolaan keamanan siber sebagai bagian dari manajemen risiko. Namun, keamanan siber masih sering dipandang sebagai persoalan teknis unit teknologi informasi, bukan sebagai tanggung jawab strategis direksi. [2]Kondisi ini menunjukkan perlunya memperjelas konstruksi tanggung jawab hukum direksi dalam tata kelola keamanan siber perusahaan digital.

Berbagai penelitian di Indonesia dalam sepuluh tahun terakhir telah membahas keamanan siber dan tata kelola perusahaan dari perspektif yang beragam. Wijayanti dan Natalia (2024) mengkaji kemampuan *security incident response* dalam mengelola insiden siber pada perusahaan,[3]. Penelitian Fattah (2026) secara lebih spesifik mengembangkan model tata kelola keamanan siber yang menempatkan *Board of Directors* sebagai aktor strategis dalam mengintegrasikan tata kelola teknologi informasi, manajemen risiko, dan

[1] Shofie Azizah et al., "Keamanan Siber Sebagai Fondasi Pengembangan Aplikasi Keuangan Mobile: Studi Literatur Mengenai Cybercrime Dan Mitigasinya," *Akuntansi Dan Teknologi Informasi* 17, no. 2 (2024): 221–37, https://doi.org/10.24123/jati.v17i2.6409.
[2] H Eka Suaib, *Keamanan Siber Dan Perlindungan Data*, *Digital Governance: Konsep, Strategi Dan Implementasinya Di Indonesia*, vol. 89 (CV. Gita Lentera, 2025).
[3] M. C. Wijayanti. R. A. & Natalia, "Analisis Kemampuan Security Incident Response PT XXX Dalam Mengelola Insiden Siber," *Info Kript Jurnal Ilmiah Keamanan Siber Dan Kriptologi* 18, no. 1 (2024): 33–40, https://doi.org/10.56706/ik.v18i1.98.

keamanan siber.[4] Sementara itu, Arafat dan Nugraha (2026) secara khusus mengkaji tanggung jawab direksi dan komisaris setelah serangan siber dalam perspektif *fiduciary duty* dan *Business Judgment Rule* berdasarkan hukum Indonesia.[5]

Berbagai kajian tersebut menunjukkan bahwa keamanan siber telah berkembang menjadi bagian dari tata kelola dan risiko perusahaan yang memerlukan keterlibatan organ perusahaan pada tingkat strategis. Namun, kajian yang secara khusus mengonstruksikan tanggung jawab hukum direksi atas keamanan siber dalam perspektif hukum perusahaan Indonesia masih memerlukan pengembangan lebih lanjut, terutama dalam menentukan batas antara tanggung jawab direksi, kewajiban pengawasan, dan perlindungan *Business Judgment Rule*. Oleh karena itu, artikel ini menawarkan kebaruan dengan mengkaji keamanan siber sebagai bagian dari tanggung jawab hukum direksi serta merumuskan parameter hukum mengenai kewajiban pencegahan, pengawasan, dan pengendalian risiko siber dalam tata kelola perusahaan digital di Indonesia.

Berdasarkan uraian tersebut, permasalahan yang dikaji dalam penelitian ini adalah bagaimana pengaturan tanggung jawab hukum direksi atas keamanan siber dalam tata kelola perusahaan digital menurut hukum Indonesia dan bagaimana konstruksi hukum tanggung jawab direksi yang mampu menjamin kepastian hukum dalam tata kelola perusahaan digital. Sejalan dengan rumusan masalah tersebut, penelitian ini bertujuan untuk menganalisis pengaturan tanggung jawab direksi atas keamanan siber dalam tata kelola perusahaan digital menurut hukum Indonesia serta merumuskan konstruksi hukum tanggung jawab direksi yang mampu menjamin kepastian hukum dalam tata kelola perusahaan digital.

Penelitian ini menggunakan teori perusahaan (*corporate theory*) sebagai teori utama. Teori ini memandang perseroan sebagai subjek hukum yang menjalankan kehendaknya melalui organ-organ perusahaan, sehingga direksi berkedudukan sebagai organ yang bertanggung jawab atas pengurusan perseroan untuk mencapai maksud dan tujuan

[4] Anwar Fattah, "Model Tata Kelola BOD-SIGMA" (Board of Directors - Strategic Integration Governance Pada Cyber Security)," *Jurnal Teknik Elektro Uniba* 10, no. 2 (2026): 832–39, https://doi.org/10.36277/jteuniba.v10i2.1344.

[5] S. U. Arafat, M., & Nugraha, "Responsibilities of Boards of Directors and Commissioners After a Cyberattack: Fiduciary Duty and the Business Judgment Rule," *Equality : Journal of Law and Justice* 3, no. 1 (2026): 26–49, https://doi.org/10.69836/equality-jlj.v3i1.511.

perusahaan. Dalam konteks perusahaan digital, tanggung jawab tersebut mencakup pengelolaan risiko keamanan siber sebagai bagian dari tata kelola perusahaan yang efektif, berkelanjutan, dan berorientasi pada perlindungan kepentingan perseroan.[6]

Sebagai teori pendukung, penelitian ini menggunakan teori kepastian hukum untuk menganalisis kejelasan norma yang mengatur ruang lingkup tanggung jawab direksi terhadap keamanan siber. Kejelasan norma diperlukan agar terdapat ukuran hukum yang pasti mengenai kewajiban direksi dalam mengantisipasi, mengelola, dan mempertanggungjawabkan risiko keamanan siber yang dapat menimbulkan kerugian bagi perusahaan maupun pihak lain.[7]

Penelitian ini juga menggunakan konsep *fiduciary duty* sebagai landasan konseptual yang menegaskan bahwa direksi wajib menjalankan tugas pengurusan perseroan dengan loyalitas, kehati-hatian, serta mengutamakan kepentingan perseroan. Konsep tersebut digunakan untuk menilai apakah pengelolaan keamanan siber telah menjadi bagian dari kewajiban hukum direksi dalam menjalankan fungsi pengurusan perusahaan.[8]

Selain itu, konsep *business judgment rule* digunakan untuk menganalisis batas-batas pertanggungjawaban direksi terhadap keputusan bisnis yang berkaitan dengan kebijakan keamanan siber. Konsep ini memberikan perlindungan hukum kepada direksi atas keputusan yang diambil secara beritikad baik, berdasarkan informasi yang memadai, dilakukan dengan kehati-hatian, serta ditujukan untuk kepentingan terbaik bagi perseroan.[9]

Selanjutnya, penelitian ini menggunakan prinsip *good corporate governance* (GCG) sebagai landasan dalam mengevaluasi tata kelola perusahaan digital. Prinsip transparansi, akuntabilitas, responsibilitas, independensi, dan kewajaran menjadi parameter untuk menilai pelaksanaan tanggung jawab direksi dalam mengelola keamanan siber sebagai

[6] Hasbullah F Sjawie and L L M SH, *Direksi Perseroan Terbatas Serta Pertanggungjawaban Pidana Korporasi* (Prenada Media, 2017).
[7] A D E WARDANA, "Peran Badan Intelijen Negara Dalam Penanggulangan Tindak Pidana Siber Berbasis Kepastian Hukum" (Universitas Islam Sultan Agung, 2025).
[8] Rabbil Arya Pasyah and Ariawan Gunadi, "Penerapan Fiduciary Duty Terhadap Direksi Dalam Kasus Pencurian Aset Oleh Pekerja," *Indonesian Journal of Legality of Law* 8, no. 1 (2025): 53–57, https://doi.org/10.35965/ijlf.v8i1.7903.
[9] Angelina Ristauli Sihombing, "Analisis Komparatif Business Judgement Rule Indonesia Dan Malaysia Melindungi Direksi Dari Gugatan Pertanggungjawaban Keputusan Bisnis," *Jurnal Media Akademik (JMA)* 3, no. 12 (2025): 1–14, https://doi.org/10.62281/9pcdjw75.

bagian dari tata kelola perusahaan yang baik.[10] Keseluruhan teori, konsep, dan prinsip tersebut digunakan sebagai pisau analisis untuk mengkaji pengaturan tanggung jawab direksi atas keamanan siber sekaligus merumuskan konstruksi hukum yang mampu memberikan kepastian hukum dalam tata kelola perusahaan digital.

METODE

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk menganalisis pengaturan tanggung jawab direksi atas keamanan siber dalam tata kelola perusahaan digital serta merumuskan konstruksi hukum yang mampu memberikan kepastian hukum terhadap pelaksanaan tanggung jawab tersebut. Penelitian ini berorientasi pada kajian terhadap norma hukum positif, doktrin hukum, dan prinsip-prinsip hukum yang berkaitan dengan tata kelola perusahaan digital. Metode pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*).

Sumber bahan hukum terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer berupa Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Bahan hukum sekunder meliputi buku, jurnal ilmiah, hasil penelitian, dan pendapat para ahli yang relevan dengan objek penelitian. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, dan bahan referensi lain yang mendukung pemahaman terhadap konsep-konsep hukum yang digunakan dalam penelitian.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan cara menginventarisasi, mengidentifikasi, mengklasifikasi, dan menelaah seluruh bahan hukum yang berkaitan dengan objek penelitian. Selanjutnya, bahan hukum dianalisis melalui penafsiran gramatikal, penafsiran sistematis, dan penafsiran teleologis. Analisis tersebut dipadukan dengan penerapan asas kepastian hukum, asas itikad baik, asas kehati-hatian (*duty of care*), asas akuntabilitas, asas

[10] Daniel Rahandri et al., *Good Corporate Governance* (Minhaj Pustaka, 2025).

transparansi, asas responsibilitas, dan asas independensi sebagai dasar untuk menilai pengaturan tanggung jawab direksi atas keamanan siber serta merumuskan konstruksi hukum yang mampu mewujudkan tata kelola perusahaan digital yang adaptif dan memberikan kepastian hukum.

HASIL DAN PEMBAHASAN

Pengaturan Tanggung Jawab Direksi atas Keamanan Siber dalam Tata Kelola Perusahaan Digital Menurut Hukum Indonesia

Perkembangan teknologi informasi telah membawa perubahan mendasar dalam penyelenggaraan kegiatan usaha. Perusahaan yang sebelumnya menjalankan aktivitas bisnis secara konvensional kini semakin bergantung pada sistem elektronik dalam pengelolaan operasional, penyimpanan informasi, transaksi bisnis, serta pelayanan kepada pengguna. Kondisi tersebut tidak hanya memberikan kemudahan dalam aktivitas perusahaan, tetapi juga menghadirkan risiko baru berupa serangan siber, kebocoran data, gangguan sistem elektronik, dan penyalahgunaan informasi digital[11]. Risiko tersebut tidak lagi dapat dipandang sebagai persoalan teknis semata, melainkan telah menjadi bagian dari risiko perusahaan yang berkaitan langsung dengan keberlangsungan usaha dan perlindungan kepentingan para pihak yang memiliki hubungan hukum dengan perusahaan.

Dalam konteks hukum perusahaan, direksi memiliki kedudukan strategis sebagai organ perseroan yang bertanggung jawab atas pengurusan perusahaan. Ketentuan Pasal 1 angka 5 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas menentukan bahwa "Direksi adalah Organ Perseroan yang berwenang dan bertanggung jawab penuh atas pengurusan Perseroan untuk kepentingan Perseroan, sesuai dengan maksud dan tujuan Perseroan serta mewakili Perseroan, baik di dalam maupun di luar pengadilan sesuai dengan ketentuan anggaran dasar". Ketentuan tersebut menunjukkan bahwa kewenangan direksi tidak hanya berkaitan dengan pengambilan keputusan bisnis, tetapi juga mencakup kewajiban untuk memastikan seluruh aspek yang mendukung keberlangsungan perusahaan dapat dikelola secara efektif.

[11] Revalina Annisa Antoine et al., "Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 316–27, https://doi.org/10.61722/jmia.v2i1.3147.

Selanjutnya, Pasal 92 ayat (1) Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas mengatur bahwa "Direksi menjalankan pengurusan Perseroan untuk kepentingan Perseroan dan sesuai dengan maksud dan tujuan Perseroan". Ketentuan tersebut diperkuat oleh Pasal 97 ayat (2) Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas yang mewajibkan "Direksi berwenang menjalankan pengurusan sebagaimana dimaksud pada ayat (1) sesuai dengan kebijakan yang dipandang tepat, dalam batas yang ditentukan dalam Undang-Undang ini dan/atau anggaran dasar". Apabila direksi melakukan kesalahan atau kelalaian dalam menjalankan tugasnya yang mengakibatkan kerugian bagi perseroan, maka berdasarkan Pasal 97 ayat (3**)** Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas menyatakan "Setiap anggota Direksi bertanggung jawab penuh secara pribadi atas kerugian Perseroan apabila yang bersangkutan bersalah atau lalai menjalankan tugasnya sesuai dengan ketentuan sebagaimana dimaksud pada ayat (2)". Namun demikian, **Pasal 97 ayat (5)** Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas mengatur Pasal 97 ayat (5) Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas mengatur bahwa anggota Direksi tidak dapat dimintai pertanggungjawaban atas kerugian Perseroan sebagaimana dimaksud dalam Pasal 97 ayat (3), apabila dapat membuktikan bahwa: (a) kerugian tersebut bukan disebabkan oleh kesalahan atau kelalaiannya; (b) telah melakukan pengurusan dengan itikad baik dan kehati-hatian untuk kepentingan Perseroan serta sesuai dengan maksud dan tujuan Perseroan; (c) tidak memiliki benturan kepentingan, baik secara langsung maupun tidak langsung, atas tindakan pengurusan yang mengakibatkan kerugian; dan (d) telah mengambil tindakan untuk mencegah timbul atau berlanjutnya kerugian tersebut.

Melalui penafsiran gramatikal, kewajiban melakukan pengurusan perseroan tidak dapat dipahami secara terbatas hanya pada aspek administrasi, keuangan, atau kegiatan bisnis secara langsung. Pengurusan perseroan memiliki cakupan yang lebih luas, yaitu seluruh tindakan yang diperlukan untuk mencapai tujuan perusahaan dan menjaga keberlangsungan usaha. Dalam konteks perusahaan digital, pengelolaan keamanan siber merupakan bagian dari aktivitas pengurusan karena keberlangsungan operasional perusahaan sangat bergantung pada keamanan sistem elektronik yang digunakan. Oleh karena itu, kewajiban direksi tidak hanya mencakup pencapaian keuntungan perusahaan,

tetapi juga memastikan tersedianya sistem pengendalian yang mampu mengantisipasi risiko digital.[12]

Pemaknaan tersebut diperkuat melalui penafsiran sistematis terhadap Pasal 15 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Pasal 15 ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menunjukkan bahwa keamanan sistem elektronik merupakan kewajiban hukum bagi setiap pihak yang memanfaatkan teknologi informasi dalam kegiatan usaha. Apabila dikaitkan dengan kedudukan direksi sebagai pihak yang menjalankan pengurusan perseroan, maka tanggung jawab terhadap keamanan sistem elektronik menjadi bagian dari kewajiban direksi dalam memastikan perusahaan menjalankan kegiatan usahanya secara aman dan berkelanjutan.

Penguatan kewajiban tersebut juga terlihat dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 3 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menentukan bahwa "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya". Selain itu, Pasal 39 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan "Penyelenggara Agen Elektronik wajib memiliki dan menjalankan prosedur standar pengoperasian yang memenuhi prinsip pengendalian pengamanan data pengguna dan Transaksi Elektronik". Ketentuan tersebut menunjukkan bahwa keamanan informasi merupakan elemen penting dalam penyelenggaraan aktivitas digital perusahaan.

Dalam kaitannya dengan perlindungan data, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga memberikan kewajiban kepada pengendali data pribadi untuk menjaga keamanan data yang diproses. Pasal 35 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menentukan bahwa "Pengendali Data

[12] Mar'a Elthaf Ilahiyah and M A SE, *Corporate Governance Dan Strategic Information System* (Banyumas: wawasan Ilmu, 2025).

Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan: (a) penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan (b) penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi". Selanjutnya, Pasal 36 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyatakan "Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi", sedangkan Pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur bahwa "Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: (a) Subjek Data Pribadi; dan (b) lembaga kewajiban pemberitahuan apabila terjadi kegagalan pelindungan data pribadi".

Melalui penafsiran teleologis, keseluruhan ketentuan tersebut menunjukkan bahwa pengaturan mengenai tanggung jawab direksi dalam perusahaan digital bertujuan untuk menciptakan tata kelola perusahaan yang mampu menghadapi perkembangan teknologi sekaligus memberikan perlindungan terhadap kepentingan perusahaan dan pihak-pihak yang berkaitan dengan kegiatan usaha. Keamanan siber tidak lagi hanya menjadi kewajiban bagian teknologi informasi, tetapi merupakan bagian dari kebijakan strategis perusahaan yang berada dalam ruang lingkup pengurusan direksi.[13]

Dalam menjalankan fungsi tersebut, direksi dituntut untuk mengambil keputusan secara hati-hati, berdasarkan informasi yang memadai, serta mempertimbangkan risiko yang mungkin timbul bagi perusahaan. Oleh karena itu, penerapan kebijakan keamanan siber harus dilakukan melalui perencanaan yang jelas, pengawasan yang berkelanjutan, pengendalian internal yang memadai, serta mekanisme penanganan insiden yang efektif.[14] Apabila direksi telah menjalankan kewajibannya secara sungguh-sungguh dan mengambil

[13] Dana Indra Sensuse, Prasetyo Adi Wibowo Putro, and Eko Yon Handri, *Keamanan Siber: Pengantar Dari Sudut Pandang Sistem Informasi* (Yogyakarta: Penerbit Andi, 2026).
[14] Ilfa Damayanti Andini Harahap, Fauzi Arif Lubis, and Purnama Ramadani Silalahi, "Strategi Manajemen Risiko Dalam Upaya Meningkatkan Keamanan Siber Di Dinas Komunikasi Dan Informatika Provinsi Sumatera Utara," *Jurnal Riset Akuntansi* 4, no. 2 (2026): 87–105, https://doi.org/10.54066/jura-itb.v4i2.3817.

langkah yang diperlukan untuk mencegah kerugian, maka keputusan bisnis yang diambil tetap harus dinilai berdasarkan proses pengambilan keputusan, bukan semata-mata berdasarkan hasil akhir yang terjadi.[15]

Berdasarkan uraian tersebut, tanggung jawab direksi atas keamanan siber memiliki dasar normatif yang berkaitan dengan pengurusan perseroan, penyelenggaraan sistem elektronik, dan perlindungan data pribadi. Meskipun belum diatur secara khusus sebagai kewajiban direksi, keamanan siber merupakan bagian penting dari pengelolaan perusahaan digital karena berkaitan dengan keberlangsungan usaha, perlindungan aset digital, dan kepastian hukum.

Konstruksi Hukum Tanggung Jawab Direksi dalam Menjamin Kepastian Hukum Tata Kelola Perusahaan Digital

Perkembangan perusahaan digital telah mengubah karakter pengurusan perseroan. Perusahaan tidak lagi hanya mengandalkan aset berwujud sebagai modal utama kegiatan usaha, tetapi juga bergantung pada sistem elektronik, data, dan infrastruktur digital. Kondisi tersebut menyebabkan keamanan siber menjadi bagian penting dalam pengelolaan perusahaan karena gangguan terhadap sistem elektronik dapat memengaruhi keberlangsungan usaha, reputasi perusahaan, serta kepentingan para pihak yang memiliki hubungan hukum dengan perseroan.[16] Oleh karena itu, diperlukan konstruksi hukum yang mampu memberikan batas yang jelas mengenai kewajiban dan tanggung jawab direksi dalam mengelola risiko keamanan siber.

Dalam hukum perseroan, direksi merupakan organ yang menjalankan fungsi pengurusan perusahaan. Pasal 1 angka 5 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas menentukan bahwa direksi merupakan organ perseroan yang berwenang dan bertanggung jawab penuh atas pengurusan perseroan untuk kepentingan perseroan sesuai dengan maksud dan tujuan perseroan. Ketentuan tersebut menunjukkan

[15] Gerald Partogi Siahaan et al., "Akibat Hukum Kepailitan Perseroan Terbatas Yang Diakibatkan Perbuatan Melawan Hukum Yang Dilakukan Oleh Direksi," *Locus Journal of Academic Literature Review* 3, no. 3 (2024): 251–65, https://doi.org/10.56128/ljoalr.v3i3.292.

[16] Ismail Darmawan and Muharman Lubis, "Menghadapi Tantangan Keamanan Siber Pada Infrastruktur Kritis: Solusi Hukum Dan Etika," *Al-Adl: Jurnal Hukum* 18, no. 1 (2026): 34–53, https://doi.org/10.31602/al-adl.v18i1.19925.

bahwa direksi memiliki kedudukan sentral dalam menentukan kebijakan strategis perusahaan, termasuk kebijakan yang berkaitan dengan pengelolaan risiko digital.

Selanjutnya, Pasal 92 ayat (1) Undang-Undang Perseroan Terbatas menyatakan bahwa direksi menjalankan pengurusan perseroan untuk kepentingan perseroan dan sesuai dengan maksud serta tujuan perseroan. Ketentuan tersebut harus dimaknai secara dinamis karena aktivitas perusahaan saat ini tidak dapat dilepaskan dari penggunaan teknologi informasi. Melalui penafsiran gramatikal, istilah "pengurusan Perseroan" mencakup seluruh tindakan yang diperlukan untuk memastikan perusahaan dapat menjalankan kegiatan usahanya secara efektif, aman, dan berkelanjutan.[17] Dengan demikian, pengelolaan keamanan siber merupakan bagian dari kewajiban pengurusan direksi karena berkaitan langsung dengan keberlangsungan perusahaan.

Pemaknaan tersebut diperkuat melalui penafsiran sistematis dengan menghubungkan kewajiban direksi dalam Undang-Undang Perseroan Terbatas dengan ketentuan mengenai penyelenggaraan sistem elektronik. Pasal 15 ayat (1) Undang-Undang Nomor 12 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya". Selanjutnya, Pasal 15 ayat (2) Undang-Undang Nomor 12 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan bahwa "Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya".

Hubungan norma tersebut menunjukkan bahwa perusahaan yang menjalankan aktivitas berbasis digital memiliki kewajiban hukum untuk memastikan keamanan sistem elektronik yang digunakan.[18] Dalam konteks perseroan, kewajiban tersebut tidak dapat dilepaskan dari tanggung jawab direksi sebagai organ yang memiliki kewenangan untuk menetapkan kebijakan, mengendalikan kegiatan perusahaan, dan memastikan terselenggaranya pengelolaan risiko secara memadai.

[17] Agus Riyanto et al., *Hukum Perusahaan Indonesia* (CV. Edu Akademi, 2026).
[18] Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal USM Law Review* 7, no. 1 (2024): 333–47, https://doi.org/10.26623/julr.v7i1.8705.

Konstruksi tersebut juga berkaitan dengan Pasal 97 ayat (2) Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas yang menyatakan "Pengurusan sebagaimana dimaksud pada ayat (1), wajib dilaksanakan setiap anggota Direksi dengan itikad baik dan penuh tanggung jawab". Ketentuan ini menunjukkan bahwa tanggung jawab direksi tidak hanya dinilai berdasarkan hasil akhir dari suatu keputusan, tetapi juga berdasarkan proses pengambilan keputusan dan tindakan yang dilakukan dalam menjalankan kewenangannya. Dalam konteks keamanan siber, direksi tidak dibebani kewajiban untuk menjamin bahwa perusahaan tidak pernah mengalami serangan siber, tetapi wajib menunjukkan bahwa telah dilakukan langkah yang wajar untuk mengidentifikasi, mencegah, dan mengurangi risiko tersebut.[19]

Selanjutnya, Pasal 97 ayat (5) Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas menentukan bahwa "Anggota Direksi tidak dapat dipertanggungjawabkan atas kerugian sebagaimana dimaksud pada ayat (3) apabila dapat membuktikan: a. kerugian tersebut bukan karena kesalahan atau kelalaiannya; b. telah melakukan pengurusan dengan itikad baik dan kehati-hatian untuk kepentingan dan sesuai dengan maksud dan tujuan Perseroan; c. tidak mempunyai benturan kepentingan baik langsung maupun tidak langsung atas tindakan pengurusan yang mengakibatkan kerugian; dan d. telah mengambil tindakan untuk mencegah timbul atau berlanjutnya kerugian tersebut". Direksi dapat terbebas dari tanggung jawab apabila mampu membuktikan bahwa kerugian bukan disebabkan oleh kesalahan atau kelalaiannya, telah melakukan pengurusan dengan kehati-hatian, tidak memiliki benturan kepentingan, serta telah mengambil tindakan untuk mencegah terjadinya kerugian. Ketentuan ini menunjukkan bahwa penilaian terhadap tindakan direksi harus mempertimbangkan standar kewajaran dalam pengambilan keputusan bisnis.

Dalam perusahaan digital, standar tersebut mengharuskan direksi membangun sistem pengelolaan keamanan siber yang terencana. Kewajiban tersebut meliputi penyusunan kebijakan keamanan informasi, pembentukan mekanisme pengawasan, pengendalian akses terhadap sistem elektronik, evaluasi risiko teknologi informasi, serta penyediaan prosedur

[19] Monica Puspa Dewi Suganda Putri et al., *Hukum Bisnis Kontemporer* (Sada Kurnia Pustaka, 2025).

penanganan insiden siber.[20] Langkah-langkah tersebut merupakan bentuk tanggung jawab direksi dalam menjaga kepentingan perseroan dan mencegah terjadinya kerugian yang dapat diperkirakan.

Konstruksi tanggung jawab tersebut juga harus dikaitkan dengan perlindungan data pribadi. Pasal 35 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyatakan "Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan: a. penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan b. penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi". . Selanjutnya, Pasal 36 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyatakan "Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi", sedangkan Pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyatakan "Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: a. Subjek Data Pribadi; dan b. lembaga mengatur kewajiban pemberitahuan apabila terjadi kegagalan pelindungan data pribadi. Dalam perusahaan digital, kewajiban tersebut menjadi bagian dari tanggung jawab strategis direksi karena berkaitan dengan kepercayaan publik dan keberlangsungan hubungan hukum antara perusahaan dengan pengguna layanan.[21]

Melalui penafsiran teleologis, berbagai ketentuan tersebut bertujuan membangun tata kelola perusahaan yang mampu beradaptasi dengan perkembangan teknologi sekaligus memberikan perlindungan hukum bagi perusahaan dan pihak yang berkepentingan. Oleh karena itu, konstruksi hukum tanggung jawab direksi tidak dapat hanya berorientasi pada

[20] Habib Ferian Fajar, Afdhal Fadhila, and Muhammad Kevin Yades, "Redesain Kebijakan Hukum Keamanan Dan Ketahanan Siber: Studi Kasus Serangan Siber Pada Pusat Data Nasional Tahun 2024," *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 285–314, https://doi.org/10.33331/rechtsvinding.v14i2.2155.

[21] Ahmad Haris Junaidi, Wicipto Setiadi, and Kaharuddin Kaharuddin, "Optimalisasi Fungsi Jaringan Dokumentasi Dan Informasi Hukum Nasional Dalam Pengamanan Siber Terhadap Dokumen Dan Informasi Hukum Nasional," *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 253–270, https://doi.org/10.33331/rechtsvinding.v14i2.2211.

pertanggungjawaban setelah terjadinya kerugian, tetapi harus membangun standar perilaku yang harus dipenuhi sejak tahap perencanaan, pengawasan, dan pengendalian risiko keamanan siber.[22]

Dengan konstruksi tersebut, tanggung jawab direksi dalam perusahaan digital harus menyeimbangkan kewenangan mengambil keputusan bisnis dengan kewajiban melindungi kepentingan perseroan. Setiap keputusan terkait keamanan siber harus didasarkan pada informasi yang memadai, pertimbangan risiko, dan dapat dipertanggungjawabkan secara hukum. Konstruksi ini memberikan kepastian mengenai kewajiban direksi sekaligus perlindungan bagi direksi yang menjalankan tugasnya secara bertanggung jawab..

SIMPULAN

Pengaturan tanggung jawab direksi atas keamanan siber dalam tata kelola perusahaan digital menunjukkan bahwa kewajiban direksi tidak hanya berkaitan dengan pengelolaan kegiatan usaha secara konvensional, tetapi juga mencakup pengendalian risiko digital yang dapat memengaruhi keberlangsungan perseroan. Keamanan siber merupakan bagian dari fungsi pengurusan direksi karena berkaitan dengan keandalan sistem elektronik, perlindungan data, dan kepentingan para pihak yang berhubungan dengan perusahaan.

Konstruksi hukum tanggung jawab direksi dalam perusahaan digital perlu menempatkan keamanan siber sebagai bagian dari kebijakan strategis perusahaan melalui pengelolaan risiko, pengawasan sistem elektronik, dan tindakan pencegahan terhadap gangguan digital. Pertanggungjawaban direksi harus dinilai berdasarkan proses pengambilan keputusan dan upaya pengendalian risiko yang dilakukan dalam menjalankan fungsi pengurusan perseroan.

Oleh karena itu perusahaan perlu mengintegrasikan keamanan siber ke dalam tata kelola dan manajemen risiko sebagai bagian dari tanggung jawab direksi. Selain itu, diperlukan penguatan regulasi yang lebih spesifik mengenai standar kewajiban direksi dalam mengelola risiko keamanan siber guna memberikan kepastian hukum bagi perusahaan digital dan perlindungan terhadap seluruh pihak yang berkepentingan.

[22] Pasyah and Gunadi, "Penerapan Fiduciary Duty Terhadap Direksi Dalam Kasus Pencurian Aset Oleh Pekerja."

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan bantuan dalam pelaksanaan penelitian serta penyusunan manuskrip ini. Apresiasi disampaikan kepada pihak yang telah memberikan dukungan akademik, fasilitas, masukan ilmiah, dan kontribusi pemikiran selama proses penelitian hingga penyelesaian artikel ini. Penulis juga menghargai berbagai bentuk bantuan dan diskusi yang telah mendukung penyempurnaan substansi maupun kualitas penulisan manuskrip. Seluruh dukungan yang diberikan menjadi bagian penting dalam proses penyelesaian penelitian ini.

DAFTAR PUSTAKA

Antoine, Revalina Annisa, Najalya Siti Farizqa, Alifia Hafizha Hasna, and Masta Pasaribu. "Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)." *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 316–27. https://doi.org/10.61722/jmia.v2i1.3147.

Arafat, M., & Nugraha, S. U. "Responsibilities of Boards of Directors and Commissioners After a Cyberattack: Fiduciary Duty and the Business Judgment Rule." *Equality : Journal of Law and Justice* 3, no. 1 (2026): 26–49. https://doi.org/10.69836/equality-jlj.v3i1.511.

Azizah, Shofie, Zava Nurruzzuhrotil Ula, Dwi Mutiara, and Michelle Prajna Prameswari. "Keamanan Siber Sebagai Fondasi Pengembangan Aplikasi Keuangan Mobile: Studi Literatur Mengenai Cybercrime Dan Mitigasinya." *Akuntansi Dan Teknologi Informasi* 17, no. 2 (2024): 221–37. https://doi.org/10.24123/jati.v17i2.6409.

Darmawan, Ismail, and Muharman Lubis. "Menghadapi Tantangan Keamanan Siber Pada Infrastruktur Kritis: Solusi Hukum Dan Etika." *Al-Adl: Jurnal Hukum* 18, no. 1 (2026): 34–53. https://doi.org/10.31602/al-adl.v18i1.19925.

Fajar, Habib Ferian, Afdhal Fadhila, and Muhammad Kevin Yades. "Redesain Kebijakan Hukum Keamanan Dan Ketahanan Siber: Studi Kasus Serangan Siber Pada Pusat Data Nasional Tahun 2024." *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 285–314. https://doi.org/10.33331/rechtsvinding.v14i2.2155.

Fattah, Anwar. "Model Tata Kelola BOD-SIGMA" (Board of Directors - Strategic Integration Governance Pada Cyber Security)." *Jurnal Teknik Elektro Uniba* 10, no. 2 (2026): 832–39. https://doi.org/10.36277/jteuniba.v10i2.1344.

Harahap, Ilfa Damayanti Andini, Fauzi Arif Lubis, and Purnama Ramadani Silalahi. "Strategi Manajemen Risiko Dalam Upaya Meningkatkan Keamanan Siber Di Dinas Komunikasi Dan Informatika Provinsi Sumatera Utara." *Jurnal Riset Akuntansi* 4, no. 2 (2026): 87–105. https://doi.org/10.54066/jura-itb.v4i2.3817.

Ilahiyah, Mar'a Elthaf, and M A SE. *Corporate Governance Dan Strategic Information System*. Banyumas: wawasan Ilmu, 2025.

Junaidi, Ahmad Haris, Wicipto Setiadi, and Kaharuddin Kaharuddin. "Optimalisasi Fungsi Jaringan Dokumentasi Dan Informasi Hukum Nasional Dalam Pengamanan Siber Terhadap Dokumen Dan Informasi Hukum Nasional." *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 253–270. https://doi.org/10.33331/

rechtsvinding.v14i2.2211.

Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7, no. 1 (2024): 333–47. https://doi.org/10.26623/julr.v7i1.8705.

Pasyah, Rabbil Arya, and Ariawan Gunadi. "Penerapan Fiduciary Duty Terhadap Direksi Dalam Kasus Pencurian Aset Oleh Pekerja." *Indonesian Journal of Legality of Law* 8, no. 1 (2025): 53–57. https://doi.org/10.35965/ijlf.v8i1.7903.

Putri, Monica Puspa Dewi Suganda, M Kn SH, Kurniawan Tri Wibowo, and M H SH. *Hukum Bisnis Kontemporer*. Sada Kurnia Pustaka, 2025.

Rahandri, Daniel, Fida Arumingtyas, Seleman Hardi Yahawi, Muhammad Abdul Rosid, Siti Noor Khikmah, Anita Rinawati, Ria Puspitasari, Rijal Ibnu Sani, Arry Patria Surya Azhar, and Sukma Uli Nuha. *Good Corporate Governance*. Minhaj Pustaka, 2025.

Riyanto, Agus, Triyono Adi Saputro, Widi Wiranti, Lathifah Hanim, Erika Wulandari, Herniati Herniati, Susanto Susanto, Angrian Permana, Mirza Amelia, and Putra Halomoan. *Hukum Perusahaan Indonesia*. CV. Edu Akademi, 2026.

Sensuse, Dana Indra, Prasetyo Adi Wibowo Putro, and Eko Yon Handri. *Keamanan Siber: Pengantar Dari Sudut Pandang Sistem Informasi*. Yogyakarta: Penerbit Andi, 2026.

Siahaan, Gerald Partogi, Sunarmi Sunarmi, Budiman Ginting, and Mahmul Siregar. "Akibat Hukum Kepailitan Perseroan Terbatas Yang Diakibatkan Perbuatan Melawan Hukum Yang Dilakukan Oleh Direksi." *Locus Journal of Academic Literature Review* 3, no. 3 (2024): 251–65. https://doi.org/10.56128/ljoalr.v3i3.292.

Sihombing, Angelina Ristauli. "Analisis Komparatif Business Judgement Rule Indonesia Dan Malaysia Melindungi Direksi Dari Gugatan Pertanggungjawaban Keputusan Bisnis." *Jurnal Media Akademik (JMA)* 3, no. 12 (2025): 1–14. https://doi.org/10.62281/9pcdjw75.

Sjawie, Hasbullah F, and L L M SH. *Direksi Perseroan Terbatas Serta Pertanggungjawaban Pidana Korporasi*. Prenada Media, 2017.

Suaib, H Eka. *Keamanan Siber Dan Perlindungan Data*. *Digital Governance: Konsep, Strategi Dan Implementasinya Di Indonesia*. Vol. 89. CV. Gita Lentera, 2025.

WARDANA, A D E. "Peran Badan Intelijen Negara Dalam Penanggulangan Tindak Pidana Siber Berbasis Kepastian Hukum." Universitas Islam Sultan Agung, 2025.

Wijayanti. R. A. & Natalia, M. C. "Analisis Kemampuan Security Incident Response PT XXX Dalam Mengelola Insiden Siber." *Info Kript Jurnal Ilmiah Keamanan Siber Dan Kriptologi* 18, no. 1 (2024): 33–40. https://doi.org/10.56706/ik.v18i1.98.