AHKAM
Jurnal Hukum Islam dan Humaniora

p-ISSN: 2964-6332
e-ISSN: 2964-6340

Terindeks: Dimensions, Scilit, Lens, Semantic, Crossref Garuda, Google, Base, etc.

https://doi.org/10.58578/ahkam.v5i3.10266

CYBER-DUTY OF CARE: KERANGKA HUKUM PERTANGGUNGJAWABAN LEMBAGA ARBITRASE INTERNASIONAL ATAS PELANGGARAN KEAMANAN DATA DALAM PERSIDANGAN VIRTUAL DI INDONESIA

Cyber-Duty of Care: Legal Framework for the Liability of International Arbitration Institutions for Data Security Breaches in Virtual Hearings in Indonesia

Afandono Cahyo Putranto, Fakhrul Ardiyan,Irvandi, Riski Ari Wibowo, Diani Sadiawati
Universitas Pembangunan Nasional "Veteran" Jakarta
2510622046@mahasiswa.upnvj.ac.id; fakh.ard97@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Apr 10, 2026	May 8, 2026	May 20, 2026	May 25, 2026

Abstract

The increasing adoption of virtual conferencing technology after the COVID-19 pandemic has encouraged the use of online hearings in arbitration proceedings, while also giving rise to risks of confidential data leakage and cybersecurity breaches in transnational commercial disputes. This study aims to analyze the legal framework for the liability of international arbitration institutions for data security breaches in virtual hearings in Indonesia and to reconstruct relevant legal doctrines for the national arbitration regime. This study uses a normative juridical method with statutory, conceptual, and comparative approaches based on functional comparison. The results show that there is no legally binding standardization of cybersecurity protocols for international arbitration institutions in Indonesia, unlike Singapore and the United Kingdom, which already have more comprehensive regulatory frameworks. In addition, the construction of arbitral civil liability in the Indonesian legal system remains

AHKAM is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

fragmented and has not been able to address losses resulting from data breaches in transnational commercial disputes. The conclusion of this study affirms the need to reconstruct the concept of Cyber-Duty of Care as a new legal doctrine in the Indonesian arbitration regime that systematically integrates the principles of personal data protection, cybersecurity standards, and arbitral civil liability. These findings provide a theoretical contribution to the development of arbitration law and data protection in virtual hearings, as well as practical implications for policymakers and arbitration institutions in strengthening data security protocols in international arbitration proceedings in Indonesia.

Keywords: International Arbitration; Cyber-Duty of Care; Data Security; Legal Liability; Virtual Hearings.

Abstrak: Meningkatnya adopsi teknologi konferensi virtual pascapandemi COVID-19 telah mendorong penggunaan persidangan daring dalam proses arbitrase, sekaligus memunculkan risiko kebocoran data rahasia dan pelanggaran keamanan siber dalam sengketa komersial transnasional. Penelitian ini bertujuan untuk menganalisis kerangka hukum pertanggungjawaban lembaga arbitrase internasional atas pelanggaran keamanan data dalam persidangan virtual di Indonesia serta merekonstruksi doktrin hukum yang relevan bagi rezim arbitrase nasional. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif berbasis komparasi fungsional. Hasil penelitian menunjukkan bahwa belum terdapat standardisasi protokol keamanan siber yang bersifat mengikat secara hukum bagi lembaga arbitrase internasional di Indonesia, berbeda dengan Singapura dan Inggris yang telah memiliki kerangka pengaturan lebih komprehensif. Selain itu, konstruksi tanggung jawab perdata arbiter dalam sistem hukum Indonesia masih terfragmentasi dan belum mampu menjangkau kerugian akibat pelanggaran data dalam sengketa komersial transnasional. Simpulan penelitian ini menegaskan perlunya rekonstruksi konsep *Cyber-Duty of Care* sebagai doktrin hukum baru dalam rezim arbitrase Indonesia yang mengintegrasikan prinsip perlindungan data pribadi, standar keamanan siber, dan tanggung jawab perdata arbiter secara sistematis. Temuan ini memberikan kontribusi teoretis bagi pengembangan hukum arbitrase dan perlindungan data dalam persidangan virtual, serta implikasi praktis bagi pembuat kebijakan dan lembaga arbitrase dalam memperkuat protokol keamanan data pada proses arbitrase internasional di Indonesia.

Kata Kunci: Arbitrase Internasional; *Cyber-Duty of Care*; Keamanan Data; Pertanggungjawaban Hukum; Persidangan Virtual.

PENDAHULUAN

Revolusi digital yang berlangsung secara masif dalam dua dekade terakhir telah mengubah secara fundamental paradigma penyelenggaraan aktivitas hukum, termasuk di dalamnya pelaksanaan persidangan dan proses penyelesaian sengketa (Pramono, 2022). Transformasi ini semakin dipercepat secara dramatis oleh pandemi COVID-19 yang melanda dunia sejak akhir tahun 2019 dan secara paksa mendorong berbagai institusi, termasuk lembaga peradilan dan arbitrase, untuk mengalihkan mekanisme persidangannya ke platform

virtual. Teknologi konferensi daring seperti Zoom, Microsoft Teams, WebEx, dan platform serupa tidak lagi sekadar menjadi instrumen pendukung administratif, melainkan bertransformasi menjadi sarana primer pelaksanaan sidang yang bersifat substantif dan mengikat secara hukum (Mahpudin, 2021). Adopsi masif teknologi ini pada awalnya didorong oleh kebutuhan mendesak untuk menjaga kelangsungan sistem hukum di tengah pembatasan mobilitas fisik yang ketat, namun seiring berjalannya waktu, praktik persidangan virtual terbukti menawarkan efisiensi dan aksesibilitas yang tidak dapat diabaikan (Sihite & Marpaung, 2022). Di Indonesia, tren ini tercermin nyata dalam perkembangan regulasi dan praktik peradilan, di mana Mahkamah Agung telah menerbitkan berbagai peraturan yang mengakomodasi pelaksanaan sidang jarak jauh, sementara lembaga-lembaga arbitrase nasional dan internasional yang beroperasi di Indonesia turut menyesuaikan prosedur mereka dengan realitas baru tersebut (Ratnasari, 2023). Persidangan virtual kini bukan lagi pengecualian melainkan telah menjadi komponen integral dari lanskap sistem hukum Indonesia yang terus berevolusi (Lorenza et al., n.d.).

Penggunaan teknologi konferensi virtual dalam konteks persidangan di Indonesia telah memberikan manfaat yang sangat signifikan bagi seluruh pemangku kepentingan dalam sistem keadilan (Sachrudin & Listyowati, 2021). Para pencari keadilan, khususnya pihak-pihak yang terlibat dalam sengketa arbitrase internasional, kini dapat mengikuti persidangan tanpa harus menempuh perjalanan lintas kota atau lintas negara yang memakan biaya dan waktu yang tidak sedikit. Bagi lembaga arbitrase internasional yang menangani sengketa dengan para pihak dari berbagai negara, persidangan virtual secara signifikan mengurangi biaya operasional dan memungkinkan penyelenggaraan sidang yang lebih fleksibel menyesuaikan zona waktu berbeda. Data menunjukkan bahwa lembaga arbitrase terkemuka seperti *Singapore International Arbitration Centre* (SIAC), *International Chamber of Commerce* (ICC), dan Badan Arbitrase Nasional Indonesia (BANI) mencatat peningkatan substansial dalam penerapan sidang virtual pascapandemi, dengan proporsi yang terus bertahan bahkan setelah pemulihan kondisi pandemi (Farid, 2025). Di sisi regulasi domestik, kebijakan persidangan elektronik yang diimplementasikan melalui Peraturan Mahkamah Agung (PERMA) Nomor 7 Tahun 2022 tentang Pedoman Penyelenggaraan Persidangan secara Elektronik menjadi tonggak penting yang mengakui keabsahan persidangan virtual dalam sistem hukum Indonesia. Namun demikian, kemudahan dan efisiensi yang ditawarkan persidangan virtual ini hadir bersama dengan kompleksitas hukum baru yang belum sepenuhnya terselesaikan,

terutama berkaitan dengan aspek perlindungan data dan keamanan informasi yang dipertukarkan dalam proses persidangan tersebut.

Perkembangan teknologi informasi yang begitu pesat sebagaimana diuraikan di atas ternyata berbanding lurus dengan kemunculan konsekuensi hukum yang semakin kompleks dan serius, khususnya dalam domain perlindungan data pribadi dan keamanan informasi (Sitorus, 2023). Setiap sesi persidangan virtual yang diselenggarakan oleh lembaga arbitrase internasional melibatkan transmisi, penyimpanan, dan pemrosesan data dalam volume yang sangat besar, mencakup dokumen-dokumen kontraktual yang bersifat rahasia, laporan keuangan perusahaan, informasi strategis bisnis, keterangan saksi ahli, dan berbagai bukti elektronik yang memiliki nilai komersial dan hukum yang tinggi. Konsep perlindungan data pribadi dalam konteks ini tidak dapat dimaknai secara sempit hanya sebagai perlindungan atas informasi identitas perorangan semata, melainkan harus dipahami secara luas mencakup perlindungan atas seluruh informasi rahasia yang dipertukarkan dalam proses arbitrase, termasuk data korporasi yang bersifat *confidential* dan *commercially sensitive* (Argiansyah & Prawira, 2024). Ancaman terhadap keamanan data dalam persidangan virtual bersifat multidimensi, mulai dari serangan siber eksternal yang menargetkan platform konferensi, intersepsi transmisi data oleh pihak ketiga yang tidak berwenang, kebocoran data melalui perangkat yang tidak aman yang digunakan oleh para arbiter atau pihak berperkara, hingga risiko yang bersumber dari kelalaian prosedural dalam pengelolaan berkas perkara secara elektronik. Studi yang dilakukan oleh berbagai lembaga keamanan siber global menunjukkan bahwa platform konferensi virtual termasuk dalam kategori target serangan siber yang paling rentan, terutama ketika digunakan untuk membahas informasi bernilai tinggi sebagaimana yang lazim terjadi dalam persidangan arbitrase komersial internasional (Hardjomuljadi & others, 2026). Dengan demikian, konsekuensi perlindungan data dan keamanan informasi dalam persidangan virtual arbitrase bukan sekadar persoalan teknis semata, melainkan telah berkembang menjadi isu hukum fundamental yang menuntut kerangka regulasi yang komprehensif dan dapat ditegakkan secara efektif.

Krusialnya persoalan perlindungan data dalam konteks arbitrase internasional semakin tampak nyata ketika kita mencermati kedudukan dan karakteristik khusus dari data serta bukti-bukti yang diserahkan kepada lembaga arbitrase (Savitri et al., 2025). Dalam setiap proses arbitrase komersial internasional, para pihak lazimnya menyerahkan dokumen-dokumen yang sangat sensitif yang bilamana jatuh ke tangan pihak yang tidak berwenang dapat mengakibatkan kerugian bisnis yang sangat signifikan, mencakup di antaranya strategi

negosiasi perusahaan, data keuangan yang belum dipublikasikan, informasi mengenai inovasi teknologi yang belum dipatenkan, serta rincian hubungan kontraktual dengan mitra bisnis strategis (Rabbani & Suherman, 2023). Prinsip *confidentiality* atau kerahasiaan merupakan salah satu pilar fundamental dalam hukum arbitrase internasional yang membedakannya dari persidangan pengadilan yang bersifat publik, dan prinsip ini secara inheren mengandung kewajiban perlindungan data yang harus dijunjung tinggi oleh semua pihak yang terlibat dalam proses arbitrase (Demirer et al., 2024). Namun demikian, ketika persidangan dialihkan ke medium virtual, batas-batas kerahasiaan tersebut menjadi semakin kabur dan rentan terhadap pelanggaran yang dapat terjadi karena berbagai sebab, baik yang disengaja maupun yang bersifat kelalaian teknis dari pihak penyelenggara arbitrase (Natasha Dachi & Urbanisasi, 2025). Lembaga arbitrase internasional sebagai pengelola dan penyelenggara proses persidangan memiliki posisi yang sangat strategis dan kritis dalam ekosistem perlindungan data ini, karena merekalah yang bertanggung jawab atas infrastruktur teknologi yang digunakan, kebijakan keamanan yang diterapkan, serta pelatihan dan pengawasan terhadap seluruh personel yang memiliki akses terhadap data perkara (Teramura & Trakman, 2024). Ketika terjadi pelanggaran keamanan data yang mengakibatkan tersebarnya informasi rahasia para pihak berperkara, pertanyaan mendasar yang muncul adalah sejauh mana lembaga arbitrase dan para arbiter dapat dimintai pertanggungjawaban hukum atas kerugian yang timbul, dan bagaimana mekanisme pertanggungjawaban tersebut seharusnya dikonstruksikan secara normatif.

Kompleksitas permasalahan perlindungan data dalam arbitrase virtual semakin diperparah oleh kemungkinan terjadinya kesilapan atau kelalaian yang dilakukan oleh lembaga arbitrase internasional maupun arbiter secara individual dalam penanganan data dan berkas perkara elektronik (Tian, 2017). Kelalaian tersebut dapat termanifestasi dalam berbagai bentuk, mulai dari penggunaan platform konferensi yang tidak memiliki enkripsi end-to-end yang memadai, penyimpanan berkas perkara pada server yang tidak memenuhi standar keamanan yang dipersyaratkan, kegagalan dalam mengimplementasikan prosedur verifikasi identitas yang ketat untuk mencegah akses tidak sah dalam sesi persidangan virtual, hingga ketiadaan protokol yang jelas mengenai penanganan dan penghapusan data perkara setelah proses arbitrase selesai (Ashady et al., 2024). Dalam konteks hukum arbitrase internasional, pertanyaan mengenai pertanggungjawaban arbiter merupakan wilayah yang sangat kompleks dan belum sepenuhnya terselesaikan, karena di satu sisi terdapat tradisi pemberian imunitas kepada arbiter yang dianalogikan dengan imunitas yudisial (Muñoz &

Barocio, 2026), sementara di sisi lain terdapat perkembangan pemikiran hukum yang semakin mengakui kemungkinan pertanggungjawaban arbiter atas kerugian yang timbul dari pelanggaran kewajiban-kewajiban spesifik yang melekat pada jabatan mereka (Tampubolon, 2019). Pelanggaran data dalam persidangan virtual, bilamana dapat dibuktikan merupakan akibat dari kelalaian arbiter atau lembaga arbitrase, seharusnya dapat membuka pintu bagi mekanisme pertanggungjawaban perdata yang memungkinkan para pihak yang dirugikan untuk mendapatkan kompensasi yang memadai (Brantes et al., 2023). Persoalan ini menjadi semakin mendesak ketika melihat pada nilai sengketa yang kerap sangat besar dalam arbitrase komersial internasional, di mana kebocoran informasi rahasia dapat mengakibatkan kerugian komersial yang bersifat masif dan sulit untuk dipulihkan melalui mekanisme hukum yang ada saat ini.

Pada tataran pengaturan internasional, *UNCITRAL Model Law on International* Commercial Arbitration yang menjadi acuan utama dalam pengembangan hukum arbitrase di berbagai negara sesungguhnya tidak secara eksplisit mengatur kewajiban perlindungan data atau keamanan siber bagi lembaga arbitrase. Kekosongan normatif ini pada level instrumen internasional mencerminkan kenyataan bahwa *UNCITRAL Model Law* disusun pada era sebelum digitalisasi persidangan arbitrase mencapai skala yang sebagaimana kita saksikan dewasa ini, sehingga tidak mengantisipasi kebutuhan regulasi mengenai keamanan siber dan perlindungan data digital yang kini menjadi persoalan kritis. Meskipun demikian, UNCITRAL telah berupaya mengisi kekosongan ini melalui berbagai instrument pelengkap, termasuk UNCITRAL *Technical Notes on Online Dispute Resolution* yang memberikan panduan mengenai penyelenggaraan penyelesaian sengketa secara daring, meskipun dokumen ini tidak bersifat mengikat secara hukum dan cakupannya masih terbatas. Di tingkat lembaga arbitrase internasional, respons terhadap kebutuhan pengaturan keamanan siber dalam persidangan virtual mulai berkembang melalui berbagai regulasi internal yang disusun secara mandiri oleh masing-masing institusi, namun fragmentasi dan ketidakseragaman dalam pendekatan yang digunakan menimbulkan kesenjangan perlindungan yang signifikan. Perkembangan ini menuntut pengkajian yang mendalam dan sistematis mengenai bagaimana standar keamanan siber seharusnya dikonstruksikan secara normatif untuk memberikan perlindungan yang efektif bagi para pihak yang menggunakan layanan arbitrase virtual, sekaligus menciptakan kepastian hukum bagi lembaga arbitrase dan para arbiter dalam menjalankan fungsi mereka.

Jika kita mencermati pengaturan internal dari beberapa lembaga arbitrase internasional terkemuka, terdapat variasi yang cukup signifikan dalam pendekatan yang

mereka ambil terkait keamanan data dan perlindungan informasi rahasia. *Singapore International Arbitration Centre* (SIAC) telah mengembangkan kerangka yang relatif komprehensif melalui SIAC *Rules* 2016 dan berbagai panduan prosedural yang diterbitkan kemudian, yang mewajibkan penggunaan platform komunikasi yang aman dan mengatur prosedur penanganan dokumen elektronik dalam persidangan virtual. *International Chamber of Commerce* (ICC) melalui ICC *Rules of Arbitration* 2021 dan ICC *Cybersecurity Protocol for International Arbitration* yang diterbitkan pada tahun 2022 telah mengambil langkah lebih maju dengan menetapkan protokol keamanan siber yang lebih terperinci, mencakup panduan penggunaan enkripsi, manajemen kata sandi, penyimpanan data yang aman, dan prosedur respons insiden keamanan siber. *London Court of International Arbitration* (LCIA) melalui LCIA *Rules* 2020 juga telah memuat ketentuan yang mengakui kebutuhan perlindungan kerahasiaan dalam lingkungan digital, termasuk kewajiban bagi para pihak dan arbiter untuk menggunakan saluran komunikasi yang aman dalam pertukaran dokumen perkara. Dari perspektif hukum domestik, Singapura telah membangun kerangka hukum yang relatif kuat melalui kombinasi antara *International Arbitration Act*, *Personal Data Protection Act* (PDPA) 2012 dan berbagai amandemennya, serta panduan teknis yang dikeluarkan oleh Komisi Perlindungan Data Pribadi Singapura yang secara spesifik mencakup konteks penyelesaian sengketa. Sementara itu, Inggris sebagai yurisdiksi arbitrase terkemuka telah memiliki kerangka perlindungan data yang kuat melalui UK *General Data Protection Regulation* (UK GDPR) dan *Data Protection Act* 2018, yang berlaku secara langsung terhadap kegiatan pemrosesan data dalam proses arbitrase dan memberikan hak-hak substantif bagi subjek data yang dirugikan akibat pelanggaran keamanan data.

Dalam konteks hukum Indonesia, situasi yang dihadapi memperlihatkan kesenjangan yang cukup mencolok dibandingkan dengan perkembangan pengaturan yang terjadi pada level internasional dan di beberapa yurisdiksi asing tersebut. Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa (UU Arbitrase), yang hingga saat ini masih menjadi lex specialis dalam bidang arbitrase di Indonesia, sama sekali tidak memuat konstruksi pengaturan mengenai kewajiban perlindungan data pribadi atau keamanan siber dalam proses arbitrase, suatu kondisi yang dapat dimaklumi mengingat undang-undang tersebut disusun jauh sebelum era digitalisasi persidangan. Meskipun Indonesia telah mengambil langkah maju yang signifikan dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang berfungsi sebagai *lex generalis* dalam bidang perlindungan data, keberadaan regulasi umum ini

saja tidak mencukupi untuk mengisi kekosongan normatif dalam konteks spesifik arbitrase yang memiliki karakteristik dan kebutuhan perlindungan yang sangat khusus. Ketiadaan ketentuan *lex specialis* dalam UU Arbitrase yang secara eksplisit mengatur kewajiban lembaga arbitrase dan arbiter dalam menjaga keamanan data perkara menciptakan ketidakpastian hukum yang nyata, terutama ketika terjadi insiden pelanggaran keamanan data yang mengakibatkan kerugian bagi para pihak berperkara. Ketidakpastian ini semakin diperparah oleh kenyataan bahwa konsep pertanggungjawaban arbiter dalam sistem hukum Indonesia belum dikonstruksikan secara jelas dan komprehensif, khususnya dalam hal pertanggungjawaban perdata atas kerugian yang timbul dari kegagalan dalam menjaga kerahasiaan dan keamanan data perkara. Kondisi ini secara kolektif memunculkan kebutuhan mendesak akan upaya penemuan hukum yang sistematis untuk merekonstruksi kerangka normatif yang memadai dalam menghadapi tantangan perlindungan data dan keamanan siber dalam arbitrase virtual di Indonesia.

Berdasarkan uraian latar belakang permasalahan yang telah dipaparkan secara sistematis di atas, penelitian ini berupaya untuk menjawab dua rumusan masalah fundamental yang saling berkaitan satu sama lain. Pertama, bagaimana standarisasi protokol keamanan siber yang bersifat mengikat bagi lembaga arbitrase internasional untuk menjamin integritas proses litigasi dapat dikonstruksikan dalam sistem hukum Indonesia, dengan mengacu pada perkembangan regulasi internasional dan praktik terbaik yang telah diterapkan di berbagai yurisdiksi dan lembaga arbitrase terkemuka? Kedua, sejauh mana tanggung jawab perdata arbiter dan institusi arbitrase terhadap kerugian akibat kebocoran data rahasia dalam sengketa komersial transnasional dapat dikonstruksikan dan ditegakkan dalam kerangka hukum Indonesia yang berlaku saat ini, dan bagaimana rekonstruksi normatif yang dibutuhkan untuk mengisi berbagai celah hukum yang ada? Kedua rumusan masalah ini dipilih secara cermat karena keduanya merepresentasikan dua dimensi yang saling komplementer dalam upaya membangun kerangka hukum yang komprehensif: dimensi preventif berupa standarisasi protokol yang bersifat mengikat, dan dimensi korektif berupa mekanisme pertanggungjawaban yang dapat ditegakkan secara efektif. Jawaban atas kedua pertanyaan ini diharapkan mampu menghadirkan kontribusi normatif yang signifikan berupa rekonstruksi konsep Cyber-Duty of Care sebagai doktrin hukum baru dalam rezim arbitrase Indonesia, yang mengintegrasikan prinsip-prinsip perlindungan data pribadi, standar keamanan siber, dan tanggung jawab perdata arbiter dalam satu kerangka yang kohesif dan dapat diterapkan secara praktis oleh lembaga-lembaga arbitrase yang beroperasi dalam yurisdiksi Indonesia.

METODE

Penelitian ini menggunakan metode penelitian yuridis normatif, yakni suatu metode penelitian hukum yang memusatkan kajiannya pada norma-norma hukum positif melalui analisis bahan-bahan hukum primer, sekunder, dan tersier yang relevan dengan permasalahan yang diteliti (Marzuki, 2017). Penelitian ini menggabungkan tiga pendekatan secara sinergis: pertama, pendekatan perundang-undangan (*statute approach*), yang mengkaji seluruh peraturan perundang-undangan yang berkaitan dengan arbitrase, perlindungan data pribadi, dan keamanan siber di Indonesia—mencakup UU No. 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta berbagai peraturan pelaksana terkait—sekaligus mengkaji instrumen internasional relevan seperti *UNCITRAL Model Law on International Commercial Arbitration*, ICC *Cybersecurity Protocol for International Arbitration* 2022, SIAC *Rules* 2016, dan LCIA *Rules* 2020; kedua, pendekatan konseptual (*conceptual approach*), yang membangun dan merekonstruksi konsep-konsep hukum fundamental yang relevan seperti *duty of care, cyber-duty of care, data breach liability*, dan pertanggungjawaban perdata arbiter dengan bersumber pada doktrin-doktrin hukum yang berkembang dalam kepustakaan hukum arbitrase internasional, hukum siber, dan hukum perdata komparatif; dan ketiga, pendekatan komparatif berbasis komparasi fungsional (*functional comparative approach*), yang membandingkan kerangka hukum perlindungan data dalam konteks arbitrase antara Indonesia, Singapura—dengan instrumen utamanya berupa *International Arbitration Act* (Cap 143A), *Personal Data Protection Act* 2012 dan amandemennya 2020, serta Model *Clauses on Data Protection in Arbitration* yang dikeluarkan oleh PDPC Singapura—dan Inggris—dengan instrumen utamanya berupa UK GDPR, *Data Protection Act* 2018, dan *Arbitration Act* 1996 serta praktik *common law* yang berkembang di dalamnya—bukan sekadar membandingkan teks hukum secara formal, melainkan menganalisis fungsi hukum yang sesungguhnya dijalankan dalam masing-masing sistem. Teknik pengumpulan data yang digunakan adalah studi kepustakaan (*library research*), yakni dengan menginventarisasi, mengidentifikasi, dan menganalisis bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan atau tribunal yang relevan. Adapun teknik analisis data yang dipergunakan adalah analisis deskriptif-preskriptif, di mana setelah melakukan deskripsi yang sistematis terhadap norma-norma hukum yang berlaku dan konsep-konsep doktrin yang relevan, penelitian ini kemudian merumuskan proposisi-

proposisi preskriptif mengenai bagaimana hukum seharusnya dikonstruksikan untuk mengisi celah normatif yang teridentifikasi.

HASIL

Absennya Standarisasi Protokol Keamanan Siber yang Bersifat Mengikat bagi Lembaga Arbitrase Internasional di Indonesia dan Rekonstruksi Doktrin *Cyber-Duty of Care*

Penelitian ini menemukan bahwa Indonesia menghadapi defisit regulasi yang substansial dan signifikan dalam hal standarisasi protokol keamanan siber yang bersifat mengikat bagi lembaga arbitrase internasional. Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa sama sekali tidak memuat ketentuan yang secara spesifik mengatur kewajiban keamanan siber atau perlindungan data digital dalam penyelenggaraan arbitrase, sedangkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang berfungsi sebagai *lex generalis* tidak mampu secara optimal mengisi kekosongan normatif tersebut tanpa adanya adaptasi sektoral yang spesifik. Kondisi ini berbeda secara fundamental dengan Singapura yang memiliki tiga pilar kerangka hukum komprehensif — yakni *International Arbitration Act* (IAA), *Personal Data Protection Act* (PDPA) 2012 beserta amandemen 2020 yang mengikat lembaga arbitrase secara langsung, dan panduan teknis PDPC — serta Inggris yang menerapkan UK GDPR *Article* 32 secara penuh kepada lembaga arbitrase dengan mewajibkan enkripsi, sistem pemantauan keamanan berkala, dan *mandatory breach notification* kepada *Information Commissioner's Office* (ICO) dalam waktu 72 jam. Analisis komparatif penelitian juga menunjukkan bahwa ICC *Cybersecurity Protocol* 2022 dan SIAC *Rules* 2016 memang telah mengatur standar minimum keamanan siber, namun tingkat kemengikatannya masih bersifat prosedural-kontraktual, sementara di Indonesia bahkan standar sukarela seperti itu belum terintegrasi ke dalam regulasi sektoral manapun.

Merespons kekosongan normatif tersebut, penelitian merekonstruksi doktrin *Cyber-Duty of Care* Arbitrase sebagai doktrin hukum baru yang mengoperasionalisasikan kewajiban keamanan siber melalui tiga lapisan yang saling melengkapi secara hierarkis. Lapisan pertama adalah kewajiban preventif (*prevention layer*) yang mencakup implementasi enkripsi *end-to-end*, autentikasi multi-faktor, sertifikasi platform konferensi virtual berbasis ISO/IEC 27001, dan penunjukan petugas keamanan data (*Data Protection Officer*). Lapisan kedua adalah kewajiban

deteksi dan respons (*detection and response layer*) yang mencakup sistem pemantauan keamanan secara *real-time*, prosedur respons insiden yang terdokumentasi, dan kewajiban pelaporan insiden kepada lembaga berwenang dalam batas waktu yang ditentukan. Lapisan ketiga adalah kewajiban pemulihan (*recovery layer*) yang mencakup prosedur kompensasi bagi pihak yang dirugikan, pemulihan data, dan evaluasi pasca-insiden yang sistematis untuk mencegah pengulangan pelanggaran. Konsep ini dikonstruksikan mengadaptasi kerangka *duty of care* tiga tahap dari yurisprudensi Inggris — *proximity*, *foreseeability*, dan *justice, fairness, and reasonableness test* — ke dalam konteks spesifik kewajiban keamanan siber lembaga arbitrase, dan dapat diimplementasikan melalui revisi UU Nomor 30 Tahun 1999, penerbitan peraturan pemerintah sektoral, atau pembentukan protokol keamanan siber nasional bagi lembaga arbitrase yang mengadopsi standar ICC *Cybersecurity Protocol* 2022 dengan penyesuaian terhadap konteks hukum dan kelembagaan Indonesia.

Fragmentasi dan Ketidakmemadaian Konstruksi Pertanggungjawaban Perdata Arbiter dalam Hukum Indonesia serta Rekonstruksi Model Tiga Tingkat Pertanggungjawaban

Penelitian menemukan bahwa konstruksi pertanggungjawaban perdata arbiter dan institusi arbitrase dalam sistem hukum Indonesia masih terfragmentasi dan belum mampu menjangkau kerugian akibat pelanggaran data dalam sengketa komersial transnasional. UU Arbitrase tidak secara eksplisit mengatur batasan imunitas arbiter maupun kondisi-kondisi yang membuka pertanggungjawaban perdata mereka, sehingga sistem hukum Indonesia menghadapi tiga celah fundamental: pertama, ketiadaan pembedaan yang jelas antara pertanggungjawaban institusional lembaga arbitrase dan pertanggungjawaban personal arbiter; kedua, ketiadaan mekanisme pembuktian yang adaptif untuk kasus pelanggaran siber yang bersifat teknis dan kompleks; dan ketiga, keterbatasan dalam mengakui serta mengkompensasikan kerugian imateriil dan kerugian komersial jangka panjang yang bersifat spekulatif. Kondisi ini sangat berbeda dari Singapura yang menerapkan uji dua tahap *Spandeck Test* (*proximity* dan *policy considerations*) dalam mengkonstruksikan *duty of care* lembaga arbitrase atas keamanan data, serta Inggris yang telah memiliki UK GDPR *Article* 82 yang secara langsung memberikan hak kompensasi bagi pihak yang dirugikan akibat pelanggaran data — termasuk pengakuan kerugian imateriil seperti *distress* dan kehilangan kendali atas informasi sebagaimana ditegaskan dalam putusan *Vidal-Hall v Google Inc* [2015].

Sebagai respons atas ketiadaan kerangka yang jelas tersebut, penelitian merekonstruksi model tiga tingkat pertanggungjawaban yang terstruktur secara hierarkis. Tingkat pertama adalah pertanggungjawaban institusional primer lembaga arbitrase sebagai pengendali data yang bertanggung jawab penuh atas seluruh aspek keamanan data dalam persidangan virtual, dengan dasar pertanggungjawaban bersumber dari kombinasi kewajiban kontraktual berdasarkan Pasal 1234 dan 1239 KUHPerdata, prinsip perbuatan melanggar hukum berdasarkan Pasal 1365 KUHPerdata, dan ketentuan UU PDP. Tingkat kedua adalah pertanggungjawaban personal arbiter yang bersifat subsidier dan hanya dapat ditegakkan bilamana pelanggaran keamanan data secara langsung disebabkan oleh tindakan atau kelalaian personal arbiter dalam kapasitas non-adjudikatif — misalnya ketika arbiter menggunakan perangkat pribadi yang tidak aman untuk mengakses berkas perkara — dengan mempertahankan imunitas hanya untuk tindakan yang murni bersifat *quasi-judicial*. Tingkat ketiga adalah pertanggungjawaban vendor teknologi sebagai pemroses data yang berlaku proporsional berdasarkan kontribusi kausal mereka terhadap terjadinya pelanggaran. Penelitian juga merekomendasikan adaptasi prinsip *material contribution* dari yurisprudensi Inggris untuk mengatasi kesulitan pembuktian kausalitas dalam kasus pelanggaran siber yang kompleks, di mana penggugat cukup membuktikan bahwa kelalaian tergugat secara substansial berkontribusi terhadap terjadinya kerugian — bukan sebagai satu-satunya penyebab. Model ini memerlukan reformasi legislatif komprehensif berupa revisi UU Nomor 30 Tahun 1999 dengan penambahan bab khusus mengenai arbitrase digital, penerbitan peraturan pemerintah yang mengatur standar minimum keamanan siber bagi penyelenggara arbitrase, serta pengembangan yurisprudensi yang mengadopsi standar pembuktian kausalitas yang lebih fleksibel.

PEMBAHASAN

Standarisasi Protokol Keamanan Siber yang Bersifat Mengikat bagi Lembaga Arbitrase Internasional untuk Menjamin Integritas Proses Litigasi

Standarisasi protokol keamanan siber yang bersifat mengikat bagi lembaga arbitrase internasional pada hakikatnya merupakan konstruksi normatif yang menempatkan keamanan siber sebagai bagian integral dari kewajiban hukum yang melekat pada penyelenggara persidangan arbitrase. Doktrin *duty of care* dalam hukum perdata, yang berkembang pesat sejak putusan landmark House of Lords Inggris dalam perkara Donoghue v. Stevenson [1932] AC

562, menjadi fondasi teoritis yang relevan untuk memahami kewajiban lembaga arbitrase dalam konteks perlindungan data digital.(Wahanze, 2023) Dalam perkembangannya, doktrin *duty of care* kemudian mengalami perluasan makna seiring dengan transformasi digital masyarakat modern, memunculkan apa yang dalam literatur hukum siber kontemporer mulai dikenal sebagai *cyber-duty of care*, yakni kewajiban hukum yang secara spesifik mensyaratkan pelaku pemrosesan data untuk menerapkan standar keamanan siber yang memadai sebanding dengan risiko yang ditimbulkan oleh kegiatan pemrosesan data tersebut (Wahanze, 2023). Penerapan konsep ini dalam konteks lembaga arbitrase internasional sangat relevan mengingat karakteristik khusus dari data yang dikelola dalam proses arbitrase, yang mencakup informasi bisnis yang sangat sensitif dan bernilai tinggi dari para pihak berperkara (Gordon, 2026). Standarisasi protokol keamanan siber yang mengikat diperlukan untuk mengoperasionalisasikan kewajiban hukum ini ke dalam bentuk norma yang konkret, terukur, dan dapat dipaksakan melalui mekanisme hukum yang ada (Gidron & Volovelsky, 2022). Dengan demikian, analisis mengenai standarisasi protokol ini harus dilakukan secara komprehensif dengan mempertimbangkan perkembangan di tingkat internasional, praktik lembaga arbitrase terkemuka, dan kondisi kerangka hukum di berbagai yurisdiksi yang relevan.

Pada tataran regulasi lembaga arbitrase internasional, ICC telah mengambil posisi terdepan dalam upaya standarisasi keamanan siber melalui penerbitan ICC *Cybersecurity Protocol for International Arbitration* pada tahun 2022 yang merupakan dokumen panduan komprehensif pertama yang khusus ditujukan untuk mengatasi risiko keamanan siber dalam proses arbitrase internasional (Łągiewska, 2024). Protokol ICC tersebut mengidentifikasi beberapa komponen standar minimum yang seharusnya dipenuhi dalam setiap persidangan arbitrase virtual, mencakup penggunaan enkripsi *end-to-end* dalam semua komunikasi yang berkaitan dengan perkara, implementasi sistem autentikasi multi-faktor untuk akses platform persidangan, pengelolaan data perkara melalui repositori digital yang tersertifikasi, pembatasan akses berdasarkan prinsip *need-to-know*, serta prosedur insiden respons yang terdokumentasi dengan jelas (Dmytro et al., 2025). SIAC melalui berbagai panduan prosedural yang diterbitkan bersama SIAC *Rules* 2016 beserta amandemennya juga telah menetapkan standar operasional keamanan siber yang mencakup kewajiban bagi arbiter dan para pihak untuk menggunakan saluran komunikasi yang aman, prosedur verifikasi identitas dalam sidang virtual (Appleton, 2026), serta ketentuan mengenai penyimpanan dan penghapusan data perkara yang aman. LCIA melalui LCIA *Rules* 2020 telah mengakomodasi

kebutuhan perlindungan kerahasiaan digital melalui Pasal 30 yang mengatur kewajiban kerahasiaan secara komprehensif, meskipun ketentuan teknis keamanan sibernya masih memerlukan pengembangan lebih lanjut untuk menyesuaikan dengan dinamika ancaman siber yang terus berkembang (Egan & Yu, 2022). Perbedaan mendasar antara ketiga lembaga arbitrase ini terletak pada tingkat kemengikatannya—dimana ICC *Cybersecurity Protocol* secara eksplisit dirancang sebagai pedoman yang dapat diadopsi secara sukarela atau diwajibkan melalui perjanjian para pihak, sedangkan ketentuan keamanan dalam SIAC *Rules* dan LCIA *Rules* bersifat lebih mengikat secara prosedural sebagai bagian dari rules of procedure yang disepakati para pihak ketika memilih forum arbitrase tersebut.

Singapura sebagai salah satu pusat arbitrase internasional terkemuka di dunia telah membangun kerangka hukum yang relatif paling komprehensif di kawasan Asia Pasifik dalam hal perlindungan data dalam konteks arbitrase (Neelakantan & Giorgadze, 2023). Kerangka tersebut bertumpu pada tiga pilar utama: pertama, *International Arbitration Act* (IAA) Cap. 143A yang memberikan otoritas hukum bagi pelaksanaan arbitrase internasional di Singapura sekaligus mengakui kebutuhan perlindungan kerahasiaan proses arbitrase secara umum; kedua, *Personal Data Protection Act* (PDPA) 2012 beserta amandemennya pada tahun 2020 yang secara signifikan memperkuat rezim perlindungan data di Singapura dengan memperkenalkan konsep mandatory breach notification, penguatan sanksi, serta ketentuan mengenai pemrosesan data yang bertanggung jawab; dan ketiga, panduan teknis yang dikeluarkan oleh *Personal Data Protection Commission* (PDPC) Singapura, termasuk *Advisory Guidelines on Key Concepts in the PDPA* yang secara spesifik mengklarifikasi penerapan ketentuan PDPA dalam berbagai konteks pemrosesan data, termasuk dalam penyelenggaraan proses penyelesaian sengketa (Anissa & Multazam, 2024). Yang sangat signifikan dari pengembangan kerangka hukum Singapura adalah bahwa PDPA berlaku secara langsung dan mengikat terhadap lembaga-lembaga arbitrase yang beroperasi di Singapura, termasuk SIAC dan lembaga arbitrase internasional lainnya yang menyelenggarakan persidangan di yurisdiksi Singapura, sehingga menciptakan standar perlindungan data yang berbasis hukum positif dan bukan sekadar pedoman sukarela. Komisi Perlindungan Data Singapura juga telah menerbitkan *Model Data Protection Clauses* yang dapat diadopsi oleh lembaga penyelesaian sengketa untuk menjamin pemenuhan standar PDPA dalam pengelolaan data perkara. Dari sisi sanksi, pelanggaran terhadap PDPA dapat mengakibatkan pengenaan denda yang substansial, sehingga menciptakan insentif yang kuat bagi lembaga arbitrase untuk memastikan kepatuhan terhadap standar perlindungan data yang ditetapkan.

Inggris sebagai yurisdiksi arbitrase terkemuka yang dikenal sebagai salah satu seat of arbitration paling populer di dunia telah memiliki kerangka perlindungan data yang sangat kuat pascaBritain Exit dari Uni Eropa melalui kombinasi antara UK *General Data Protection Regulation* (UK GDPR) dan Data Protection Act 2018. UK GDPR sebagai adaptasi dari EU GDPR dalam konteks hukum Inggris memuat prinsip-prinsip fundamental perlindungan data yang secara langsung relevan dengan penyelenggaraan arbitrase, termasuk prinsip purpose limitation yang membatasi penggunaan data hanya untuk tujuan yang telah ditentukan secara eksplisit, prinsip data minimisation yang mensyaratkan pengumpulan data hanya sebatas yang diperlukan, prinsip storage limitation yang mengatur retensi data, serta prinsip integrity and confidentiality yang secara langsung mewajibkan implementasi langkah-langkah keamanan teknis dan organisasional yang memadai (Zhou et al., 2023). Berdasarkan ketentuan *Article* 32 UK GDPR, setiap pengendali dan pemroses data—yang dalam konteks arbitrase mencakup lembaga arbitrase dan para arbiter—berkewajiban untuk mengimplementasikan langkah-langkah teknis dan organisasional yang sesuai untuk menjamin tingkat keamanan yang sebanding dengan risiko yang dihadapi, mencakup enkripsi data, kemampuan untuk memastikan kerahasiaan dan integritas sistem, kemampuan untuk memulihkan ketersediaan data setelah insiden, serta proses pengujian dan evaluasi keamanan secara berkala (Raymond et al., 2010). Dalam praktik, *Arbitration Act* 1996 yang menjadi landasan hukum arbitrase di Inggris telah diinterpretasikan oleh pengadilan untuk mengakomodasi kewajiban kerahasiaan yang komprehensif, termasuk dalam dimensi digital, sehingga membentuk kerangka yang saling melengkapi antara hukum arbitrase dan hukum perlindungan data. Ketentuan mandatory breach notification dalam UK GDPR yang mewajibkan pelaporan insiden keamanan data kepada *Information Commissioner's Office* (ICO) dalam waktu 72 jam juga berlaku bagi lembaga arbitrase, menciptakan mekanisme akuntabilitas yang konkret dan dapat dipaksakan (Basedow et al., 2021).

Berbeda dengan perkembangan yang terjadi di Singapura dan Inggris, kerangka hukum Indonesia dalam bidang arbitrase dan perlindungan data masih menghadirkan kesenjangan normatif yang cukup signifikan dan memerlukan rekonstruksi yang menyeluruh. UU No. 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa, meskipun telah mengatur aspek kerahasiaan proses arbitrase secara umum melalui Pasal 27 yang menyatakan bahwa semua pemeriksaan sengketa dilakukan secara tertutup, tidak memuat ketentuan apapun yang secara spesifik mengatur kewajiban keamanan siber atau perlindungan data digital dalam penyelenggaraan arbitrase. Kekosongan normatif ini tidak

dapat sepenuhnya ditutup oleh UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang berfungsi sebagai *lex generalis*, meskipun undang-undang ini telah memperkenalkan kerangka perlindungan data yang cukup komprehensif dengan mencakup kewajiban pengendali data untuk menerapkan langkah-langkah keamanan yang memadai, hak subjek data, dan sanksi atas pelanggaran (Anjheli, 2024). Persoalannya terletak pada ketiadaan ketentuan sektoral yang mengadaptasi kewajiban umum perlindungan data tersebut ke dalam konteks spesifik arbitrase, yang memiliki karakteristik unik berupa adanya prinsip kerahasiaan yang sangat ketat, keterlibatan data korporasi yang tidak termasuk dalam definisi data pribadi konvensional, dan kompleksitas yurisdiksi yang bersifat transnasional. Pemerintah Indonesia juga belum menerbitkan peraturan pelaksana dari UU PDP yang secara spesifik mengatur sektor arbitrase dan penyelesaian sengketa alternatif lainnya, sehingga lembaga arbitrase yang beroperasi di Indonesia—termasuk BANI dan berbagai lembaga arbitrase internasional yang menyelenggarakan sidang di Indonesia—beroperasi dalam kondisi ketidakpastian hukum yang cukup serius dalam hal kewajiban perlindungan data dan keamanan siber (Pebrian et al., 2025). Kondisi ini secara fundamental berbeda dari apa yang dialami oleh lembaga arbitrase yang beroperasi di Singapura atau Inggris, di mana ketentuan hukum yang lebih jelas dan komprehensif memberikan panduan yang lebih pasti mengenai standar keamanan yang harus dipenuhi.

Rekonstruksi konsep *cyber-duty of care* dalam konteks arbitrase Indonesia memerlukan pemahaman yang mendalam mengenai bagaimana doktrin ini dapat dioperasionalisasikan secara normatif dalam sistem hukum positif Indonesia. Konsep *cyber-duty of care* yang diusulkan dalam penelitian ini mengadaptasi kerangka *duty of care* tiga tahap yang dikembangkan dalam yurisprudensi Inggris—*proximity, foreseeability*, dan *the justice, fairness, and reasonableness test*—ke dalam konteks spesifik kewajiban keamanan siber lembaga arbitrase. Dalam konteks ini, elemen *proximity* terpenuhi mengingat adanya hubungan kontraktual yang jelas antara lembaga arbitrase dengan para pihak berperkara, yang menciptakan kewajiban perlindungan yang bersifat langsung dan dapat diidentifikasi. Elemen *foreseeability* terpenuhi karena risiko kebocoran data dalam persidangan virtual adalah risiko yang secara objektif dapat diduga dan seharusnya diantisipasi oleh setiap penyelenggara layanan arbitrase yang bertindak dengan tingkat kehati-hatian yang layak. Elemen *justice, fairness, and reasonableness* terpenuhi karena secara moral dan sosial sangatlah adil untuk mengharapkan lembaga arbitrase yang menerima imbalan atas jasa profesionalnya untuk menerapkan standar keamanan siber yang memadai dalam melindungi data rahasia yang dipercayakan kepada

mereka oleh para pihak. Konsep *cyber-duty of care* ini dalam kerangka hukum Indonesia dapat dikonstruksikan melalui beberapa jalur normatif yang saling melengkapi: pertama, melalui penafsiran ekstensif terhadap ketentuan kerahasiaan dalam UU Arbitrase yang mencakup dimensi kerahasiaan digital; kedua, melalui penerapan prinsip itikad baik dalam pelaksanaan perjanjian (Pasal 1338 KUHPerdata) yang mewajibkan lembaga arbitrase untuk menggunakan segala upaya yang wajar dalam menjaga keamanan data para pihak; dan ketiga, melalui penerapan ketentuan UU PDP yang mengatur kewajiban pengamanan data oleh pengendali data terhadap lembaga arbitrase sebagai pengendali data.

Sebagai ilustrasi komparatif yang sistematis, berikut disajikan tabel perbandingan komprehensif mengenai standarisasi protokol keamanan siber dalam konteks arbitrase internasional antara Indonesia, Singapura, dan Inggris beserta standar yang berlaku dalam lembaga arbitrase utama:

Tabel 1. Perbandingan Standarisasi Protokol Keamanan Siber dalam Arbitrase Internasional

Indikator	Indonesia	Singapura	Inggris	SIAC	ICC
Landasan Hukum Utama	UU No. 30/1999 (Arbitrase); UU No. 27/2022 (PDP)	IAA (Cap. 143A); PDPA 2012 (amend. 2020)	Arbitration Act 1996; UK GDPR; DPA 2018	SIAC Rules 2016; Panduan Prosedural SIAC	ICC Rules 2021; ICC Cybersecurity Protocol 2022
Kewajiban Protokol Keamanan Siber	Belum ada lex specialis; hanya norma umum dalam UU PDP	PDPA wajib berlaku; PDPC Guidelines memperkuat kewajiban sektoral	UK GDPR Art. 32 wajib berlaku penuh terhadap lembaga arbitrase	Diatur dalam panduan prosedural; mengikat sebagai bagian prosedur	ICC Cybersecurity Protocol 2022; dapat diwajibkan melalui perjanjian
Standar Enkripsi Data	Tidak diatur secara eksplisit dalam UU Arbitrase	PDPA mewajibkan langkah perlindungan yang 'reasonable'; enkripsi direkomendasikan kuat oleh PDPC	UK GDPR Art. 32 secara eksplisit menyebut enkripsi sebagai langkah teknis yang tepat	Panduan SIAC merekomendasikan komunikasi melalui saluran aman dengan enkripsi	ICC Protocol mensyaratkan enkripsi end-to-end sebagai standar minimum
Mekanisme Mandatory Breach Notification	Belum ada kewajiban khusus dalam konteks arbitrase; UU PDP mengatur	PDPA mewajibkan notifikasi kepada PDPC dan subjek data terdampak dalam 3 hari kalender	UK GDPR mewajibkan notifikasi kepada ICO dalam 72 jam dan kepada subjek data	Prosedur insiden diserahkan pada kebijakan institusi; belum distandarisasi secara formal	ICC Protocol merekomendasikan prosedur respons insiden namun belum mewajibkan notifikasi formal

Indikator	Indonesia	Singapura	Inggris	SIAC	ICC
	kewajiban umum		jika risiko tinggi		
Lembaga Pengawas	Lembaga Pengawas PDP (dalam proses pembentukan berdasarkan UU PDP)	Personal Data Protection Commission (PDPC) — aktif dan berwenang penuh	Information Commissioner's Office (ICO) — aktif dan berwenang penuh	Pengawasan internal SIAC dan PDPC Singapura (bagi operasi berbasis di Singapura)	Pengawasan internal ICC; tunduk pada regulator data yurisdiksi seat of arbitration
Sanksi Pelanggaran Keamanan Data	Pidana dan perdata berdasarkan UU PDP (denda maks. 2% dari pendapatan tahunan); belum kontekstual untuk arbitrase	Denda hingga SGD 1 juta atau 10% dari pendapatan tahunan (berdasarkan PDPA amend. 2020)	Denda hingga £17,5 juta atau 4% dari omzet global tahunan (UK GDPR)	Sanksi prosedural internal SIAC; tidak secara eksplisit mengatur tanggung jawab perdata lembaga	Sanksi prosedural internal ICC; ketentuan pertanggungjawaban perdata lembaga terbatas
Kewajiban Penunjukan Dpo/Petugas Keamanan Data	Belum diwajibkan secara spesifik untuk lembaga arbitrase dalam regulasi yang ada	Tidak diwajibkan secara universal namun sangat direkomendasikan oleh PDPC untuk organisasi yang memproses data sensitif dalam volume besar	UK GDPR mewajibkan penunjukan DPO dalam kondisi-kondisi tertentu, termasuk pemrosesan data sensitif dalam skala besar	SIAC memiliki petugas keamanan data internal; tidak secara eksplisit mewajibkan hal serupa dari para arbiter	ICC merekomendasikan penunjukan Information Security Officer dalam ICC Protocol
Ketentuan Retensi Dan Penghapusan Data	Belum ada ketentuan khusus dalam UU Arbitrase; UU PDP mengatur prinsip storage limitation secara umum	PDPA mengatur retensi data hanya selama diperlukan untuk tujuan yang diidentifikasi; panduan PDPC memberikan kejelasan lebih lanjut	UK GDPR Art. 5(1)(e) mewajibkan storage limitation; ICO memberikan panduan retensi yang rinci	SIAC mengatur prosedur pengarsipan internal; ketentuan penghapusan belum diatur secara eksplisit	ICC Protocol memuat ketentuan mengenai pengelolaan data perkara setelah arbitrase selesai
Sertifikasi Platform	Belum ada persyaratan khusus;	PDPC merekomendasikan penggunaan	ICO menerbitkan panduan	SIAC merekomendasikan platform yang	ICC Protocol memberikan kriteria teknis

Indikator	Indonesia	Singapura	Inggris	SIAC	ICC
Konferensi Virtual	hanya tunduk pada PERMA No. 7/2022 yang bersifat umum	platform yang memenuhi standar keamanan terverifikasi (ISO 27001 dsb)	mengenai penggunaan platform konferensi yang aman; tidak ada daftar platform yang wajib digunakan	aman namun belum menetapkan standar sertifikasi yang wajib	minimum untuk platform konferensi virtual; sertifikasi spesifik tidak diwajibkan
Tingkat Kemengikatan Secara Hukum	Rendah — celah normatif signifikan antara UU Arbitrase dan UU PDP	Tinggi — PDPA mengikat secara hukum terhadap lembaga arbitrase; sanksi dapat diterapkan	Sangat Tinggi — UK GDPR dan DPA 2018 mengikat penuh dengan sanksi besar; ICO aktif melakukan enforcement	Menengah — mengikat dalam kerangka prosedur SIAC namun tidak memiliki dasar hukum eksternal yang kuat	Menengah-Rendah — mengikat hanya jika disepakati para pihak; bersifat sukarela secara default

Dari analisis komparatif yang disajikan dalam tabel di atas, dapat ditarik kesimpulan bahwa Indonesia menghadapi defisit regulasi yang substansial dalam hal standarisasi protokol keamanan siber yang bersifat mengikat bagi lembaga arbitrase internasional. Novelty atau temuan baru yang dihasilkan dari penelitian ini adalah rekonstruksi konsep *Cyber-Duty of Care* Arbitrase sebagai doktrin hukum baru yang secara khusus dikonstruksikan untuk mengisi kekosongan normatif dalam sistem hukum arbitrase Indonesia. Doktrin ini dioperasionalisasikan melalui tiga lapisan kewajiban yang saling melengkapi: lapisan pertama berupa kewajiban preventif (*prevention layer*) yang mencakup implementasi protokol keamanan teknis minimum yang terstandarisasi, termasuk enkripsi, autentikasi multi-faktor, dan sertifikasi platform; lapisan kedua berupa kewajiban deteksi dan respons (*detection and response layer*) yang mencakup sistem pemantauan keamanan secara real-time, prosedur respons insiden yang terdokumentasi, dan kewajiban pelaporan insiden kepada lembaga berwenang; dan lapisan ketiga berupa kewajiban pemulihan (*recovery layer*) yang mencakup prosedur pemulihan data, kompensasi bagi pihak yang dirugikan, dan evaluasi pasca-insiden untuk mencegah terulangnya pelanggaran serupa. Rekonstruksi doktrin *Cyber-Duty of Care* Arbitrase ini menawarkan model normatif yang dapat diadopsi melalui revisi terhadap UU No. 30 Tahun 1999, penerbitan peraturan pemerintah sektoral, atau melalui pembentukan peraturan Kepala Badan Arbitrase Nasional Indonesia (BANI) yang komprehensif, dengan

mengintegrasikan standar teknis keamanan siber yang setara dengan ICC Cybersecurity Protocol 2022 dan diselaraskan dengan ketentuan UU PDP yang berlaku.

Tanggung Jawab Perdata Arbiter dan Institusi Arbitrase Terhadap Kerugian Akibat Kebocoran Data Rahasia Dalam Sengketa Komersial Transnasional di Indonesia

Konstruksi pertanggungjawaban perdata arbiter dalam hukum arbitrase internasional merupakan wilayah yang secara historis diliputi ketidakpastian dan perdebatan yang cukup mendasar, mengingat adanya ketegangan yang inheren antara dua prinsip yang saling berlawanan: di satu sisi, prinsip imunitas yudisial yang secara tradisional diberikan kepada arbiter sebagai upaya melindungi kebebasan dan independensi mereka dalam pengambilan keputusan, dan di sisi lain, prinsip akuntabilitas profesional yang menghendaki setiap pelaku jasa profesional untuk bertanggung jawab atas kerugian yang timbul dari kelalaian dalam melaksanakan tugas mereka (Muñoz & Barocio, 2026). Pertanyaan mengenai pertanggungjawaban perdata arbiter dan lembaga arbitrase atas kebocoran data rahasia menambah satu dimensi kompleksitas baru dalam perdebatan tersebut, karena pelanggaran keamanan data pada dasarnya tidak berkaitan langsung dengan kualitas keputusan arbitrase yang diproteksi oleh imunitas yudisial, melainkan berkaitan dengan kewajiban pengelolaan data yang bersifat administratif dan teknis (Teramura & Trakman, 2024). Perbedaan kategorisasi ini sangat krusial karena menentukan apakah imunitas arbiter dapat atau tidak dapat diperluas untuk mencakup tindakan atau kelalaian dalam pengelolaan keamanan data. Dalam perkembangan pemikiran hukum yang lebih kontemporer, terdapat kecenderungan yang semakin kuat untuk membedakan secara tegas antara tindakan quasi-judicial yang dilindungi oleh imunitas dan tindakan administratif atau manajerial yang tidak seharusnya mendapat perlindungan imunitas yang sama (Risnain, 2018). Pelanggaran kewajiban keamanan siber dalam persidangan virtual secara argumennya masuk dalam kategori tindakan administratif-manajerial yang seharusnya dapat menjadi dasar pertanggungjawaban perdata, khususnya ketika pelanggaran tersebut disebabkan oleh kelalaian yang bersifat gross negligence atau kesengajaan.

Doktrin imunitas arbiter telah berkembang secara berbeda di berbagai sistem hukum, dan pemahaman yang tepat mengenai batasan dan pengecualian dari imunitas tersebut menjadi prasyarat fundamental dalam mengkonstruksikan pertanggungjawaban perdata arbiter atas pelanggaran keamanan data (Muñoz & Barocio, 2026; Tampubolon, 2019).

Dalam sistem hukum common law, doktrin judicial immunity yang dikembangkan melalui yurisprudensi panjang telah diterapkan secara analogi kepada arbiter dengan alasan bahwa fungsi adjudikatif yang mereka jalankan memerlukan perlindungan yang sama dengan yang diberikan kepada hakim pengadilan. Namun, batas-batas imunitas ini telah mengalami penyempitan yang signifikan melalui perkembangan yurisprudensi dan regulasi modern, dengan pengakuan yang semakin kuat bahwa imunitas hanya melindungi tindakan yang bersifat quasi-judicial dan tidak mencakup tindakan yang bersifat administratif, kontraktual, atau yang merupakan pelanggaran tugas yang bersifat non-adjudikatif. Dalam konteks Inggris, *Arbitration Act 1996* Pasal 29 memang memberikan imunitas kepada arbiter atas tanggung jawab atas tindakan atau kelalaian dalam melaksanakan fungsinya, kecuali bilamana tindakan atau kelalaian tersebut dilakukan dengan itikad buruk (*bad faith*), dan ketentuan ini telah diinterpretasikan oleh pengadilan Inggris untuk tidak mencakup kelalaian dalam pengelolaan keamanan informasi yang bersifat administratif (Ling, 2022). Di Singapura, IAA tidak secara eksplisit mengatur imunitas arbiter, namun ketentuan common law mengenai imunitas diterapkan dengan berbagai nuansa, termasuk pengakuan bahwa kelalaian dalam pengelolaan data perkara dapat membuka peluang pertanggungjawaban perdata bilamana dapat dibuktikan adanya kelalaian yang cukup berat (*gross negligence*) (Hayward, 2025).

Dalam kerangka hukum Indonesia, konstruksi pertanggungjawaban perdata arbiter dihadapkan pada kompleksitas berlapis yang bersumber dari ketiadaan ketentuan eksplisit mengenai imunitas arbiter sekaligus ketiadaan ketentuan yang mengatur pertanggungjawaban arbiter secara komprehensif dalam UU Arbitrase. Pasal 16 UU Arbitrase memang mengatur mengenai kemandirian dan ketidakberpihakan arbiter, namun tidak memberikan panduan yang jelas mengenai batasan imunitas dan kondisi-kondisi yang dapat membuka pertanggungjawaban perdata arbiter. Dalam konteks pelanggaran keamanan data, pertanggungjawaban perdata arbiter dalam sistem hukum Indonesia dapat dikonstruksikan melalui beberapa basis hukum yang berbeda: pertama, melalui konsep perbuatan melanggar hukum (*onrechtmatige daad*) sebagaimana diatur dalam Pasal 1365 KUHPerdata, bilamana dapat dibuktikan bahwa arbiter atau lembaga arbitrase melakukan tindakan atau kelalaian yang bertentangan dengan kewajiban hukum yang ada, mengakibatkan kerugian, terdapat hubungan kausalitas, dan pelaku memiliki kesalahan (*schuld*) (Ehnts, 2024; Indonesia, n.d.); kedua, melalui konsep wanprestasi atau *breach of contract* berdasarkan Pasal 1234 juncto Pasal 1239 KUHPerdata (Ramadhani, 2012), bilamana kewajiban keamanan data dapat dikonstruksikan sebagai bagian dari kewajiban kontraktual yang timbul dari perjanjian

arbitrase atau *terms of appointment* arbiter; dan ketiga, melalui penerapan ketentuan UU PDP yang mengatur pertanggungjawaban pengendali dan pemroses data atas pelanggaran yang terjadi akibat kelalaian dalam implementasi langkah-langkah keamanan yang disyaratkan. Ketiga basis hukum ini dapat berlaku secara kumulatif atau alternatif tergantung pada fakta-fakta yang dapat dibuktikan dalam kasus tertentu.

Pengalaman yurisdiksi Singapura dalam mengkonstruksikan pertanggungjawaban lembaga arbitrase atas pelanggaran data memberikan wawasan yang sangat berharga bagi pengembangan kerangka serupa di Indonesia. Dalam sistem hukum Singapura, pertanggungjawaban lembaga arbitrase atas pelanggaran keamanan data dapat dikonstruksikan melalui beberapa mekanisme yang saling melengkapi. Pertama, melalui penerapan PDPA yang secara langsung mewajibkan organisasi, termasuk lembaga arbitrase yang beroperasi di Singapura, untuk mengimplementasikan langkah-langkah keamanan yang 'reasonable' dalam melindungi data yang berada dalam penguasaannya, dengan kegagalan memenuhi kewajiban ini dapat mengakibatkan pengenaan sanksi administratif oleh PDPC sekaligus membuka peluang tuntutan perdata dari pihak yang dirugikan. Kedua, melalui doktrin *negligence* dalam hukum *tort* Singapura yang mengikuti kerangka umum yang ditetapkan dalam *Spandeck Engineering (S) Pte Ltd v Defence Science & Technology Agency* [2007] 4 SLR(R) 100, di mana pengadilan Singapura menerapkan uji dua tahap yang terdiri dari *proximity* dan *policy considerations* untuk menentukan apakah *duty of care* timbul dalam situasi tertentu, dan doktrin ini secara argumennya dapat diterapkan untuk mengkonstruksikan duty of care lembaga arbitrase atas keamanan data pihak berperkara (Gidron & Volovelsky, 2022). Ketiga, melalui ketentuan kontraktual dalam perjanjian arbitrase atau *terms of appointment* yang dapat secara eksplisit mengatur kewajiban keamanan data dan mekanisme pertanggungjawaban bilamana kewajiban tersebut dilanggar. Dari ketiga mekanisme ini, penerapan PDPA memberikan basis pertanggungjawaban yang paling kuat dan relatif paling mudah ditegakkan karena tidak memerlukan pembuktian kesalahan (fault) yang kompleks sebagaimana dipersyaratkan dalam tuntutan negligence.

Inggris, sebagai yurisdiksi yang memiliki tradisi panjang dan kaya dalam hukum arbitrase dan hukum perlindungan data, menawarkan model pertanggungjawaban yang lebih multidimensional dan terstruktur dalam menangani pelanggaran keamanan data dalam konteks arbitrase. Berdasarkan UK GDPR Article 82, setiap individu yang mengalami kerugian materiil atau imateriil sebagai akibat dari pelanggaran terhadap ketentuan UK GDPR berhak untuk memperoleh kompensasi dari pengendali data atau pemroses data yang

bertanggung jawab atas pelanggaran tersebut, dan dalam konteks arbitrase (Demirer et al., 2024), ini berarti lembaga arbitrase sebagai pengendali data utama dapat secara langsung dituntut secara perdata oleh para pihak yang datanya bocor. Perkembangan yurisprudensi di Inggris mengenai pertanggungjawaban perdata atas pelanggaran data dalam konteks profesional telah semakin mengarah pada pengakuan bahwa kerugian imateriil—seperti distress, kecemasan, dan kehilangan kontrol atas informasi pribadi—juga merupakan kerugian yang dapat dikompensasikan, sebagaimana ditegaskan dalam putusan *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 yang kemudian diterapkan lebih lanjut dalam berbagai putusan berikutnya. Dalam konteks arbitrase komersial transnasional, kategori kerugian yang dapat timbul dari pelanggaran keamanan data jauh lebih luas, mencakup kerugian komersial langsung akibat bocornya informasi rahasia kepada pihak lawan sengketa atau pihak ketiga, kerugian reputasional yang sulit diukur namun nyata dampaknya bagi perusahaan yang terlibat, serta potensi kerugian strategis jangka panjang akibat tersebarnya informasi mengenai strategi bisnis atau teknologi yang bersifat *proprietari* (Demirer et al., 2024). Ketentuan Article 82 UK GDPR juga mengatur mengenai pembagian beban tanggung jawab antara pengendali dan pemroses data, yang dalam konteks arbitrase menciptakan kerangka pertanggungjawaban yang dapat berlaku secara proporsional antara lembaga arbitrase (sebagai pengendali utama) dan platform teknologi yang digunakan (sebagai pemroses) (Rianda, 2025).

Dalam mengkonstruksikan bentuk pertanggungjawaban perdata yang tepat dalam konteks arbitrase komersial transnasional di Indonesia, penelitian ini menemukan perlunya pembedaan yang jelas antara dua lapisan pertanggungjawaban yang saling berkaitan namun berbeda dalam hal subjek dan dasar hukumnya. Lapisan pertama adalah pertanggungjawaban institusional, yakni pertanggungjawaban lembaga arbitrase sebagai entitas hukum yang menyelenggarakan proses arbitrase dan secara langsung mengelola infrastruktur teknologi serta kebijakan keamanan yang digunakan dalam persidangan virtual. Pertanggungjawaban institusional ini dapat dikonstruksikan berdasarkan: (a) ketentuan Pasal 1365 KUHPerdata mengenai perbuatan melanggar hukum bilamana lembaga arbitrase terbukti gagal memenuhi standar kehati-hatian yang wajar (*redelijkheid en billijkheid*) dalam pengelolaan keamanan data; (b) ketentuan wanprestasi berdasarkan Pasal 1234 dan 1239 KUHPerdata bilamana kewajiban keamanan data diperlakukan sebagai bagian dari kewajiban kontraktual lembaga arbitrase; dan (c) ketentuan UU PDP yang mengatur pertanggungjawaban pengendali data atas pelanggaran yang terjadi akibat kegagalan implementasi langkah-langkah keamanan yang

disyaratkan (Bintarawati, 2024; Iwanti & others, 2022; Setiadi et al., 2025). Lapisan kedua adalah pertanggungjawaban personal arbiter, yang secara konseptual lebih kompleks karena bersinggungan dengan doktrin imunitas. Dalam penelitian ini, diusulkan bahwa pertanggungjawaban personal arbiter atas pelanggaran keamanan data seharusnya dapat dikonstruksikan bilamana pelanggaran tersebut terjadi dalam kapasitas non-adjudikatif arbiter—misalnya ketika arbiter menggunakan perangkat pribadi yang tidak aman untuk mengakses berkas perkara, atau ketika arbiter secara tidak sengaja mengekspos data kepada pihak yang tidak berwenang melalui tindakan yang tidak terkait dengan fungsi quasi-judicial mereka—karena dalam kondisi tersebut imunitas yudisial seharusnya tidak berlaku.

Persoalan kompensasi dan penilaian kerugian dalam kasus pelanggaran keamanan data arbitrase juga merupakan area yang memerlukan pengembangan normatif yang signifikan dalam sistem hukum Indonesia. Kerugian yang dapat timbul dari kebocoran data rahasia dalam arbitrase komersial transnasional mencakup dimensi yang sangat luas dan seringkali sulit untuk dikuantifikasi secara akurat: kerugian materiil langsung berupa biaya remediasi dan pemulihan data, kerugian bisnis akibat hilangnya keunggulan kompetitif dari informasi yang bocor (CNN Indonesia, 2023), kerugian akibat tuntutan hukum pihak ketiga yang dapat timbul sebagai konsekuensi dari bocornya informasi, serta kerugian imateriil berupa kerusakan reputasi dan kehilangan kepercayaan pelanggan atau mitra bisnis. Dalam sistem hukum Indonesia berdasarkan KUHPerdata, prinsip ganti kerugian mengenal konsep damnum emergens (kerugian yang nyata diderita) dan lucrum cessans (keuntungan yang gagal diperoleh), dan keduanya secara teoretis dapat diterapkan dalam konteks pelanggaran keamanan data arbitrase. Namun demikian, kemampuan sistem hukum Indonesia untuk secara efektif mengkompensasi kerugian imateriil dan kerugian komersial jangka panjang yang bersifat spekulatif masih terbatas, berbeda dengan perkembangan yang terjadi di Inggris dan Singapura di mana pengadilan semakin mengakui dan mengkompensasi berbagai kategori kerugian yang timbul dari pelanggaran data secara lebih komprehensif. Untuk mengisi kesenjangan ini, penelitian ini merekomendasikan pengembangan mekanisme kompensasi khusus dalam kerangka hukum arbitrase Indonesia yang mengakui kekhususan kerugian dalam konteks pelanggaran keamanan data, termasuk kemungkinan penerapan liquidated damages atau pre-agreed compensation dalam perjanjian arbitrase yang mengatur konsekuensi spesifik dari pelanggaran kewajiban keamanan data.

Sebagai representasi komparatif yang sistematis, berikut disajikan tabel perbandingan yang memuat indikator-indikator kunci terkait dengan tanggung jawab perdata arbiter dan

institusi arbitrase atas kebocoran data rahasia dalam sengketa komersial transnasional di tiga yurisdiksi yang dikaji:

Tabel 2. Perbandingan Pertanggungjawaban Perdata Arbiter dan Institusi Arbitrase atas Kebocoran Data Rahasia

Indikator	Indonesia	Singapura	Inggris
Basis Hukum Pertanggungjawaban Perdata	Pasal 1365 KUHPerdata (PMH); Pasal 1234 & 1239 KUHPerdata (Wanprestasi); UU No. 27/2022 tentang PDP (pengendali data)	Tort of Negligence (Spandeck Test); PDPA 2012 Pasal 48J (enforcement); Contract Law (implied duty of confidentiality)	UK GDPR Art. 82 (hak kompensasi langsung); Tort of Negligence; Data Protection Act 2018 Sec. 168-169; Breach of Contract
Doktrin Imunitas Arbiter	Tidak diatur eksplisit; celah normatif yang signifikan; diterapkan secara analogi dari hukum hakim	Common law immunity berlaku; dikecualikan untuk bad faith dan tindakan non-adjudikatif; tidak dikodifikasikan dalam IAA	Arbitration Act 1996 Sec. 29 mengatur imunitas arbiter dengan pengecualian bad faith; tidak mencakup kelalaian administratif
Batasan Imunitas Dalam Konteks Pelanggaran Data	Belum ada ketentuan eksplisit; terdapat argumen kuat bahwa kelalaian keamanan siber bersifat non-adjudikatif sehingga tidak dilindungi imunitas	Imunitas tidak mencakup tindakan non-adjudikatif; kelalaian keamanan data berpotensi membuka pertanggungjawaban	Sec. 29 dikonstruksikan tidak mencakup kelalaian administratif; pelanggaran data secara konsisten dikategorikan sebagai tindakan non-adjudikatif
Standar Pembuktian Kelalaian	Beban pembuktian pada penggugat; menerapkan standar subjektif-objektif berdasarkan yurisprudensi MA RI	Dua tahap Spandeck Test: proximity + policy considerations; prinsip material contribution mulai diadopsi dalam kasus kompleks	Material contribution test; reversed burden dalam kasus tertentu berdasarkan UK GDPR Art. 82(3); standar lebih fleksibel
Jenis Kerugian Yang Dapat Dikompensasikan	Damnum emergens dan lucrum cessans (KUHPerdata); kerugian imateriil diakui namun penilaiannya tidak konsisten	Kerugian materiil dan imateriil; distress diakui dalam yurisprudensi; PDPA memungkinkan kompensasi langsung dari PDPC	Kerugian materiil dan imateriil (termasuk distress dan kehilangan kendali atas data); UK GDPR Art. 82 mengakui keduanya secara eksplisit
Mekanisme Pembebanan Ganti Kerugian	Ganti rugi berdasarkan Pasal 1246-1248 KUHPerdata; belum ada mekanisme khusus untuk pelanggaran data arbitrase	Kompensasi berdasarkan penilaian pengadilan; PDPC dapat memerintahkan pembayaran kompensasi; mediasi data breach tersedia	Kompensasi berdasarkan UK GDPR Art. 82; ICO dapat mengenakan denda; collective/group claims dimungkinkan untuk data breach masif
Pertanggungjawaban Institusi Arbitrase Vs. Arbiter Individu	Belum dibedakan secara eksplisit dalam regulasi; praktik peradilan belum	Lembaga arbitrase sebagai data controller menanggung beban pertanggungjawaban	Lembaga arbitrase sebagai data controller bertanggung jawab berdasarkan UK GDPR;

Indikator	Indonesia	Singapura	Inggris
	mengembangkan preseden yang memadai	primer berdasarkan PDPA; arbiter dapat dimintai pertanggungjawaban secara personal dalam kondisi tertentu	arbiter individu dapat dimintai pertanggungjawaban berdasarkan tort law jika kelalaiannya terbukti secara personal
Mekanisme Penyelesaian Sengketa Pelanggaran Data	Pengadilan negeri (gugatan PMH/wanprestasi); pengaduan kepada Lembaga Pengawas PDP (dalam pembentukan)	Pengadilan negeri Singapura; PDPC enforcement (investigation dan directions); mediasi melalui PDPC	Pengadilan sipil Inggris; ICO enforcement (investigations, fines, enforcement notices); Information Tribunal untuk banding
Klausul Pengecualian Tanggung Jawab Dalam Rules Arbitrase	Belum diatur dalam UU Arbitrase; dimungkinkan dalam kesepakatan para pihak namun tunduk pada prinsip ketertiban umum dan itikad baik KUHPerdata	SIAC Rules mengandung klausul pembatasan tanggung jawab institusi; efektivitasnya tunduk pada PDPA dan common law	ICC dan LCIA Rules memuat klausul pengecualian tanggung jawab; efektivitasnya dibatasi oleh UK GDPR dan Unfair Contract Terms Act 1977
Tingkat Kepastian Hukum Dalam Penerapan	Rendah — tidak ada preseden, celah regulasi signifikan, mekanisme penegakan belum berkembang	Menengah-Tinggi — PDPA memberikan kepastian yang cukup baik; yurisprudensi mulai berkembang; panduan PDPC membantu	Tinggi — UK GDPR memberikan kepastian hukum yang kuat; ICO aktif melakukan enforcement; yurisprudensi yang kaya dan berkembang

Berdasarkan keseluruhan analisis yang telah dilakukan, penelitian ini menemukan novelty berupa rekonstruksi konseptual atas kerangka pertanggungjawaban perdata arbiter dan institusi arbitrase dalam sistem hukum Indonesia. Model ini mengusulkan tiga tingkat pertanggungjawaban yang terstruktur secara hierarkis: tingkat pertama berupa pertanggungjawaban institusional primer lembaga arbitrase sebagai pengendali data yang bertanggung jawab penuh atas seluruh aspek keamanan data dalam penyelenggaraan persidangan virtual, dengan dasar pertanggungjawaban yang bersumber dari kombinasi antara kewajiban kontraktual, ketentuan UU PDP, dan prinsip perbuatan melanggar hukum; tingkat kedua berupa pertanggungjawaban personal arbiter yang bersifat subsidier dan hanya dapat ditegakkan bilamana pelanggaran keamanan data secara langsung disebabkan oleh tindakan atau kelalaian personal arbiter dalam kapasitas non-adjudikatif mereka, dengan mempertahankan imunitas arbiter hanya untuk tindakan yang murni bersifat quasi-judicial; dan tingkat ketiga berupa pertanggungjawaban vendor teknologi sebagai pemroses data yang

berlaku bilamana pelanggaran keamanan bersumber dari kegagalan platform atau infrastruktur teknologi yang digunakan dalam persidangan virtual. Model ini secara fundamental berbeda dari pendekatan yang saat ini berlaku dalam sistem hukum Indonesia yang tidak memiliki pembedaan yang jelas antara ketiga tingkat pertanggungjawaban tersebut, dan menawarkan solusi normatif yang lebih presisi, adil, dan dapat ditegakkan secara efektif dalam rangka memberikan perlindungan yang memadai bagi para pihak yang menggunakan layanan arbitrase virtual di Indonesia. Implementasi model ini memerlukan reformasi legislatif yang mencakup revisi terhadap UU No. 30 Tahun 1999 dengan menambahkan bab khusus mengenai arbitrase digital, penerbitan peraturan pemerintah yang mengatur standar keamanan siber minimum bagi penyelenggara arbitrase, serta pengembangan mekanisme sertifikasi dan audit keamanan siber yang diawasi oleh lembaga berwenang

KESIMPULAN

Penelitian ini berhasil merekonstruksi kerangka normatif standarisasi protokol keamanan siber yang bersifat mengikat bagi lembaga arbitrase internasional di Indonesia melalui pengembangan doktrin *Cyber-Duty of Care* Arbitrase. Analisis komparatif yang dilakukan terhadap sistem hukum Indonesia, Singapura, dan Inggris serta berbagai regulasi lembaga arbitrase internasional seperti ICC, SIAC, dan LCIA mengungkapkan defisit regulasi yang signifikan dalam kerangka hukum Indonesia, di mana UU No. 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa sama sekali tidak memuat ketentuan mengenai keamanan siber atau perlindungan data digital, sementara UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang berlaku sebagai lex generalis tidak mampu secara optimal mengisi kekosongan normatif tersebut tanpa adanya adaptasi sektoral yang spesifik. Novelty penelitian ini terletak pada rekonstruksi doktrin *Cyber-Duty of Care* Arbitrase yang dioperasionalisasikan melalui tiga lapisan kewajiban yang saling melengkapi secara hierarkis: lapisan preventif yang mewajibkan implementasi protokol keamanan teknis minimum terstandarisasi mencakup enkripsi end-to-end, autentikasi multi-faktor, dan sertifikasi platform; lapisan deteksi dan respons yang mewajibkan sistem pemantauan real-time, prosedur respons insiden terdokumentasi, dan mandatory breach notification kepada lembaga berwenang; serta lapisan pemulihan yang mencakup prosedur kompensasi bagi pihak yang dirugikan dan evaluasi pasca-insiden yang sistematis. Doktrin ini menawarkan model normatif yang dapat diimplementasikan melalui revisi terhadap UU Arbitrase,

penerbitan peraturan pemerintah sektoral, atau pembentukan protokol keamanan siber nasional bagi lembaga arbitrase yang mengadopsi standar ICC Cybersecurity Protocol 2022 dengan penyesuaian terhadap konteks hukum dan kelembagaan Indonesia.

Penelitian ini juga berhasil merekonstruksi konsep pertanggungjawaban perdata arbiter dan institusi arbitrase atas kerugian akibat kebocoran data rahasia dalam sengketa komersial transnasional di Indonesia melalui pengembangan model dalam arbitrase virtual. Analisis terhadap kerangka pertanggungjawaban di Singapura—yang mengandalkan kombinasi antara PDPA, *doctrine of negligence* berbasis *Spandeck Test*, dan ketentuan kontraktual—serta di Inggris—yang menerapkan UK GDPR Article 82 secara langsung dengan standar pembuktian yang lebih fleksibel dan pengakuan kerugian imateriil yang komprehensif—menunjukkan bahwa sistem hukum Indonesia menghadapi tiga celah fundamental: ketiadaan pembedaan yang jelas antara pertanggungjawaban institusional dan personal arbiter, ketiadaan mekanisme pembuktian yang adaptif untuk kasus pelanggaran siber yang kompleks, dan keterbatasan dalam mengakui dan mengkompensasikan kerugian imateriil serta kerugian komersial jangka panjang yang bersifat spekulatif. Model yang diusulkan mengkonstruksikan tiga tingkat pertanggungjawaban yang terstruktur: pertanggungjawaban institusional primer lembaga arbitrase sebagai pengendali data yang bersumber dari kombinasi kewajiban kontraktual, UU PDP, dan prinsip perbuatan melanggar hukum; pertanggungjawaban personal arbiter yang bersifat subsidier dan terbatas pada tindakan non-adjudikatif yang menyebabkan pelanggaran keamanan data, dengan mempertahankan imunitas quasi-judicial untuk tindakan adjudikatif murni; serta pertanggungjawaban vendor teknologi sebagai pemroses data yang berlaku proporsional berdasarkan kontribusi kausal mereka terhadap terjadinya pelanggaran. Implementasi efektif model ini memerlukan reformasi legislatif komprehensif yang mencakup revisi terhadap UU No. 30 Tahun 1999, penerbitan peraturan pemerintah yang mengatur standar minimum keamanan siber bagi penyelenggara arbitrase digital, dan pengembangan yurisprudensi yang mengadopsi standar pembuktian kausalitas yang lebih fleksibel berbasis prinsip material contribution, sehingga secara holistik menempatkan Indonesia pada posisi yang setara dengan Singapura dan Inggris dalam memberikan perlindungan hukum yang memadai bagi para pihak yang menggunakan layanan arbitrase virtual dalam sengketa komersial transnasional.

DAFTAR PUSTAKA

Anissa, S., & Multazam, M. T. (2024). Assessing legal measures for addressing personal data misuse in commercial settings: A critical analysis. *Indonesian Journal of Law and Economics Review, 19*(2). https://doi.org/10.21070/ijler.v19i2.1012

Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(1), 165–189. https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3964

Appleton, B. (2026). *Arbitration hacked: Toward a unified cybersecurity and data breach framework for international arbitral proceedings*. SSRN. https://doi.org/10.2139/ssrn.6625218

Argiansyah, H. Y., & Prawira, M. R. Y. (2024). Analisis Hukum Hak atas Privasi dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia. *Jurnal Hukum Pelita, 5*(1), 61–75.

Ashady, S., Grindulu, L., Islam, M. H., & Zainuddin, M. (2024). Perkembangan Regulasi dan Pelaksanaan Mediasi pada Persidangan Secara Elektronik Pasca Berlakunya Peraturan Mahkamah Agung Nomor 3 Tahun 2022. *CERMIN: Jurnal Penelitian, 8*(1), 13–29. https://doi.org/10.36841/cermin_unars.v8i1.4152

Basedow, J., Dietze, J., Griller, S., Kellerbauer, M., Klamert, M., Malferrari, L., Scharf, T., Schnichels, D., Thym, D., & Tomkin, J. (2021). European integration: Quo vadis? A critical commentary on the PSPP judgment of the German Federal Constitutional Court of May 5, 2020. *International Journal of Constitutional Law, 19*(1), 188–207. https://doi.org/10.1093/icon/moab017

Bintarawati, F. (2024). The influence of the Personal Data Protection Law (UU PDP) on law enforcement in the digital era. *ANAYASA: Journal of Legal Studies, 1*(2), 135–143. https://doi.org/10.61397/ays.v1i2.92

Brantes, F. D., Giovannini, C., Gromova, E. A., & Ferreira, J. B. (2023). Arbitration chambers and technology: Witness tampering and perceived effectiveness in videoconferenced dispute resolution proceedings. *International Journal of Law and Information Technology, 31*(1), 75–90. https://doi.org/10.1093/ijlit/eaad012

CNN Indonesia. (2023, May 22). *Kominfo Klarifikasi Soal Dugaan Bocoran Data BSI yang Beredar*. https://www.cnnindonesia.com/teknologi/20230522122857-192-952382/kominfo-klarifikasi-soal-dugaan-bocoran-data-bsi-yang-beredar

Demirer, M., Jiménez Hernández, D., Li, D., & Peng, S. (2024). *Data, privacy laws and firm production: Evidence from the GDPR* (NBER Working Paper No. 32146). National Bureau of Economic Research. https://doi.org/10.3386/w32146

Dmytro, P.-T., Volodymyr, S., Vitaliy, D., Yevheniy, R., & Volodymyr, M. (2025). Legal framework for cybersecurity in the context of the metaverse formation. *Metaverse Science, Society and Law, 1*(1). https://doi.org/10.69635/mssl.2025.1.1.18

Egan, M., & Yu, H.-L. (2022). Intersecting and dissecting confidentiality and data protection in online arbitration. *Journal of Business Law, 2022*(2), 135–163. https://dspace.stir.ac.uk/handle/1893/31758

Ehnts, D. (2024). Quo vadis, Schuldenbremse? Über Sinn und Unsinn detaillierter Defizit- und Schuldenregelungen im Grundgesetz. *Wirtschaftsdienst, 104*(1), 25–28.

Farid, A. S. (2025). Wacana Kritis Media Online terhadap Koperasi Merah Putih sebagai Proyek Ekonomi Politik Pembangunan Desa. *Jurnal Syiar-Syiar, 5*(1), 57–75.

Febriani, H., Agustina, I., Monica, S., & Adiyanto, M. R. (2023). Property rights, definition and infringement of trademarks and trade secret rights: Literature review. *Proceeding International Conference on Economy, Management, and Business, 1*(1), 198–207.

Ferreira, D. B., Giovannini, C., Gromova, E. A., & Ferreira, J. B. (2023). Arbitration chambers and technology: Witness tampering and perceived effectiveness in videoconferenced dispute resolution proceedings. *International Journal of Law and Information Technology, 31*(1), 75–90. https://doi.org/10.1093/ijlit/eaad012

Gidron, T., & Volovelsky, U. (2022). How related are the Scottish snail of 1926 and the Israeli decomposed snail of 2022: Is *Donoghue v Stevenson* still relevant in 21st century law? In *Donoghue v Stevenson—The Immortal Snail—90th Anniversary Conference Papers*. The Continuing Legal Education Society of British Columbia.

Gordon, E. (2026). *The doctrine of privity in negligence: Understanding the path to Donoghue v Stevenson*. Bloomsbury Publishing.

Hardjomuljadi, S. (2026). Pertanggungjawaban Etik Arbiter dan Implikasinya terhadap Kekuatan Putusan Arbitrase di Indonesia. *Journal of Syntax Literate, 11*(1).

Hayward, B. (2025). *Submission to the public consultation on the International Arbitration Act 1994 of Singapore and the international arbitration regime* [Law reform submission].

Indonesia. (n.d.). *Kitab Undang-Undang Hukum Perdata (KUH Perdata) Pasal 1365 tentang Perbuatan Melawan Hukum (PMH)*.

Iwanti, N. A. M., & Taun. (2022). Akibat Hukum Wanprestasi serta Upaya Hukum Wanprestasi Berdasarkan Undang-Undang yang Berlaku. *The Juris, 6*(2), 346–351. https://doi.org/10.56301/juris.v6i2.601

Łągiewska, M. (2024). *Digitalization and the use of new technologies in international arbitration*. Brill/Nijhoff.

Ling, D. T. C. (2022). Cybersecurity in international arbitration: An untapped opportunity for arbitral institutions. *Singapore Academy of Law Journal, 34*, 432–463. https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal/Current-Issue/ctl/eFirstSALPDFJournalView/mid/494/ArticleId/1783/Citation/JournalsOnlinePDF

Lorenza, A., Maharani, A. S., & Rioneldi. (n.d.). Implementasi dan Dampak bagi Advokat dalam Pelaksanaan Pendaftaran Perkara secara Virtual. *DIH: Jurnal Ilmu Hukum, 17*(1), 373650.

Mahpudin, M. (2021). Gowaslu sebagai Electoral Technology: Keterlibatan Publik dalam Pengawasan Partisipatif Berbasis Daring. *Jurnal Adhyasta Pemilu, 4*(2), 1–21. https://doi.org/10.55108/jap.v4i2.53

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media.

Muñoz, E., & Barocio, P. M. (2026). Rethinking arbitrator immunity: The role of party-arbitrator agreements. *Journal of International Arbitration, 43*(2), 173–196. https://doi.org/10.54648/joia2026008

Natasha Dachi, F., & Urbanisasi. (2025). Tanggung Jawab Perdata dalam Transaksi Crypto Asset: Kajian terhadap Risiko Kerugian Investor. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora, 3*(2), 69–79. https://doi.org/10.55606/jurrish.v3i2.5638

Neelakantan, V., & Giorgadze, V. (2023). Emergency arbitration procedures under the rules of the Singapore International Arbitration Centre (SIAC). *BCDR International Arbitration Review, 10*(2).

Pebrian, D., Amanita, A., & Ardan, R. A. R. (2025). Perbandingan Arbitrase SIAC dan BANI dalam Penyelesaian Sengketa Bisnis Berdasarkan Konvensi New York 1958. *Rechtswetenschap: Jurnal Mahasiswa Hukum, 2*(2). https://doi.org/10.36859/rechtswetenschap.v2i2.3484

Pramono, N. (2022). Perkembangan Hukum Kontrak di Era Digital. *Jurnal Hukum dan Pembangunan, 52*(2), 145–162. https://jhp.ui.ac.id/index.php/home/article/view/1890

Rabbani, R. F., & Suherman, S. (2023). Urgensi Pengaturan Confidentiality Agreement sebagai Optimalisasi Perlindungan Kerahasiaan Informasi Bernilai Ekonomi. *Jurnal USM Law Review, 6*(3), 1020–1039. https://doi.org/10.26623/julr.v6i3.7830

Ramadhani, D. A. (2012). Wanprestasi dan Akibat Hukumnya. *Jurnal Yuridis, 15*(17).

Ratnasari, W. P. (2023). Industri Budaya dan Komoditas: Studi Kasus Tenun Tradisional Nusa Tenggara Barat sebagai Komoditas dan Seni dalam Kerangka Budaya dan Religi. *Jurnal Kommunity Online, 3*(2), 201–218. https://doi.org/10.15408/jko.v3i2.31027

Raymond, C. M., Fazey, I., Reed, M. S., Stringer, L. C., Robinson, G. M., & Evely, A. C. (2010). Integrating local and scientific knowledge for environmental management. *Journal of Environmental Management, 91*(8), 1766–1777. https://doi.org/10.1016/j.jenvman.2010.03.023

Rianda, F. U. (2025). *Urgensi Pengaturan Central Bank Digital Currency untuk Melindungi Data Pribadi dari Cybercrime di Indonesia* [Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim].

Risnain, M. (2018). Eksistensi Lembaga Quasi Judisial dalam Sistem Kekuasaan Kehakiman di Indonesia: Kajian terhadap Komisi Pengawas Persaingan Usaha. *Jurnal Hukum dan Peradilan, 3*(1), 49–58. https://doi.org/10.25216/jhp.3.1.2014.49-58

Sachrudin, A., & Listyowati, P. R. (2021). Pandangan Hakim Pengadilan Agama Semarang terhadap Implementasi E-Court dalam Administrasi dan Proses Persidangan Perkara Perceraian. *Prosiding Konstelasi Ilmiah Mahasiswa Unissula (KIMU) Klaster Hukum*, 580–598. https://jurnal.unissula.ac.id/index.php/kimuh/article/view/11963

Savitri, Z. A., Amirulloh, M., & Susanto, M. (2025). Urgensi Sertifikat Keandalan Privasi dalam Menghadapi Kebocoran Data Pribadi. *Jurnal USM Law Review, 8*(1), 235–253. https://doi.org/10.26623/julr.v8i1.11385

Setiadi, R. B., Sahari, A., & Isnina, I. (2025). Penerapan Asas Perbuatan Melawan Hukum Material dalam Perspektif Hukum Tindak Pidana Korupsi di Kejaksaan. *Iuris Studia: Jurnal Kajian Hukum, 6*(1), 145–150. https://jurnal.bundamediagrup.co.id/index.php/iuris/article/view/850

Sihite, Y. A., & Marpaung, D. S. H. (2022). Efektivitas E-Court sebagai Sarana Penyelesaian Sengketa di Tengah Pandemi Covid-19 di Indonesia. *Widya Yuridika: Jurnal Hukum, 5*(1), 95–106. https://doi.org/10.31328/wy.v5i1.2495

Sitorus, S. Y. H. (2023). *Perlindungan Hukum Data Pribadi Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Ditinjau dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi* [Thesis, Universitas Kristen Indonesia].

Tampubolon, W. S. (2019). Peranan Seorang Arbiter dalam Penyelesaian Sengketa melalui Arbitrase. *Jurnal Ilmiah Advokasi, 7*(1), 21–30. https://doi.org/10.36987/jiad.v7i1.242

Teramura, N., & Trakman, L. (2024). Confidentiality and privacy of arbitration in the digital era: Pies in the sky? *Arbitration International, 40*(3), 277–306. https://doi.org/10.1093/arbint/aiae017

Tian, Y. (2017). *The impact of third-party funding on international arbitration procedures and regulatory recommendations* [Doctoral dissertation, China University of Political Science and Law].

Wahanze, R. (2023). *Examining the "neighbour principle" in Donoghue v Stevenson as a test for qualifying the duty of care element used in determining the liability of a defendant in negligent misstatements*. SSRN. https://doi.org/10.2139/ssrn.4612565

Zhou, W., Zhang, D., Han, G., Zhu, W., & Wang, X. (2023). A blockchain-based privacy-preserving and fair data transaction model in IoT. *Applied Sciences, 13*(22), Article 12389. https://doi.org/10.3390/app132212389