KEDAULATAN SIBER INDONESIA DALAM IMPLEMENTASI AUTOMATIC EXCHANGE OF INFORMATION: TINJAUAN HUKUM PELINDUNGAN DATA DAN KEAMANAN INFORMASI PERPAJAKAN

Nur Malasari[1], Hafid Zakariya[2], Ariy Khaerudin,[3]
Magister Hukum Universitas Islam Batik Surakarta
Email: nmalasari53@gmail.com

ABSTRAK

Artikel ini menganalisis konstruksi pengaturan Automatic Exchange of Information (AEOI) di Indonesia dalam perspektif kedaulatan siber serta kesesuaiannya dengan prinsip perlindungan data pribadi dan norma penyelenggaraan sistem elektronik. Ruang lingkup AEOI dalam artikel ini mencakup AEOI-CRS atas informasi rekening keuangan, Amended CRS, dan AEOI-CARF atas informasi aset kripto relevan sebagaimana dikonstruksikan dalam regulasi teknis terbaru. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan terbatas terhadap standar OECD. Bahan hukum primer meliputi UU Nomor 9 Tahun 2017, UU KUP, UU PDP, UU ITE sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024, PP Nomor 71 Tahun 2019, Perpres Nomor 82 Tahun 2022, PMK Nomor 108 Tahun 2025, PER-10/PJ/2025, CRS, Amended CRS, CARF MCAA, dan dokumen OECD mengenai confidentiality serta data safeguards. Hasil penelitian menunjukkan bahwa Indonesia memiliki legitimasi hukum yang memadai untuk melaksanakan AEOI. Namun, perluasan cakupan ke aset kripto memperbesar konsekuensi hukum terhadap transfer data lintas batas, pembatasan tujuan, kontrol akses, audit trail, keamanan sistem elektronik, dan akuntabilitas. Artikel ini menyimpulkan bahwa AEOI di Indonesia telah sesuai secara formal dengan prinsip pelindungan data pribadi, tetapi masih memerlukan penguatan substantif melalui harmonisasi norma, standar keamanan informasi yang spesifik, pembatasan pemanfaatan ulang data, dan pembagian tanggung jawab lintas aktor.

Kata kunci: kedaulatan siber; AEOI; CRS; CARF; perlindungan data pribadi; keamanan informasi perpajakan.

ABSTRACT

This article analyses the legal construction of Automatic Exchange of Information (AEOI) in Indonesia from the perspective of cyber sovereignty and its conformity with personal data protection principles and electronic system governance norms. The scope of AEOI covers AEOI-CRS for financial account information, the Amended CRS, and AEOI-CARF for relevant crypto-asset information as constructed under recent implementing regulations. This research applies normative legal research using statutory, conceptual, and limited comparative approaches to OECD standards. Primary legal materials include Law Number 9 of 2017, the General Tax Provisions and Procedures Law, the Personal Data Protection Law, the Electronic Information and Transactions Law as last amended by Law Number 1 of 2024, Government Regulation Number 71 of 2019, Presidential Regulation Number 82 of 2022, Minister of Finance Regulation Number 108 of 2025, Director General of Taxes Regulation PER-10/PJ/2025, the CRS, the Amended CRS, the CARF MCAA, and OECD documents on confidentiality and data safeguards. The findings indicate that Indonesia has sufficient legal legitimacy to implement AEOI. However, the expansion to crypto-assets increases

legal consequences concerning cross-border data transfer, purpose limitation, access control, audit trails, electronic system security, and accountability. The article concludes that AEOI implementation in Indonesia is formally compatible with personal data protection principles, but it still requires substantive strengthening through legal harmonisation, specific information security standards, limits on repeated data use, and clearer responsibility among actors.

Keywords: cyber sovereignty; AEOI; CRS; CARF; personal data protection; tax information security.

A. PENDAHULUAN

Perkembangan tata kelola perpajakan internasional dalam dua dekade terakhir menunjukkan pergeseran dari model pengawasan yang cenderung tertutup menuju rezim transparansi berbasis pertukaran informasi. Negara tidak lagi dapat mengandalkan pelaporan domestik semata karena mobilitas modal, globalisasi jasa keuangan, dan penggunaan struktur lintas yurisdiksi membuka ruang bagi penghindaran pajak.[1] Dalam konteks tersebut, pertukaran informasi menjadi instrumen penting untuk memperkuat kepatuhan wajib pajak dan menjaga penerimaan negara. Pada tahap awal, kerja sama perpajakan internasional banyak bertumpu pada exchange of information on request. Model tersebut berguna untuk memperoleh data tertentu dari yurisdiksi lain, tetapi efektivitasnya terbatas karena bergantung pada kemampuan negara peminta untuk mengidentifikasi kasus, pihak, dan informasi yang diduga tersembunyi di luar negeri. Kompleksitas transaksi lintas batas kemudian mendorong peralihan menuju pertukaran otomatis yang lebih proaktif, periodik, dan berbasis standar bersama.[2]

Automatic Exchange of Information (AEOI) merupakan bentuk konkret dari perkembangan tersebut. Melalui AEOI, informasi keuangan tertentu dikumpulkan oleh lembaga pelapor, disampaikan kepada otoritas pajak domestik, lalu dipertukarkan dengan yurisdiksi mitra berdasarkan standar yang disepakati. Dalam praktik global, AEOI dikembangkan terutama melalui Common Reporting Standard (CRS) dan instrumen kerja sama antarotoritas yang dibangun di bawah koordinasi OECD.[3] Perkembangan terbaru menunjukkan bahwa ruang lingkup AEOI tidak lagi berhenti pada

[1] Dharma Pongrekun et al., "Digital Sovereignty in the Global South: Indonesia's Cyber Governance between Global Power and National Autonomy," *Research Journal in Advanced Humanities* 7, no. 1 (2026), https://doi.org/10.58256/hprs3b27.

[2] Putri Anggia, Ani Yunita, and Fadia Fitriyanti, "Legal Justice: The Abolition of the Principle of Bank Secrecy for Tax Interests in Indonesia," *Jambura Law Review* 5, no. 2 (2023): 314 – 331, https://doi.org/10.33756/jlr.v5i2.18793.

[3] Agus Bhakti et al., "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia," *Journal of Human Security* 20, no. 1 (2024): 109 – 117, https://doi.org/10.12924/johs2024.20116.

rekening keuangan konvensional, tetapi juga bergerak ke arah aset kripto melalui Crypto-Asset Reporting Framework (CARF).

Bagi Indonesia, keterlibatan dalam AEOI memiliki dua arti penting. Pertama, partisipasi tersebut menunjukkan komitmen Indonesia untuk mengikuti standar transparansi perpajakan global. Kedua, partisipasi itu membawa konsekuensi hukum yang tidak sederhana karena data keuangan yang dipertukarkan merupakan data sensitif, diproses melalui sistem elektronik, dan bergerak lintas yurisdiksi.[4] Oleh karena itu, AEOI tidak dapat dipahami semata-mata sebagai mekanisme administratif perpajakan, melainkan juga sebagai persoalan perlindungan data, keamanan informasi, dan kedaulatan siber. Secara normatif, titik awal penting pengaturan AEOI di Indonesia adalah UU Nomor 9 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan. Undang-undang tersebut membuka dasar hukum bagi otoritas perpajakan untuk memperoleh akses terhadap informasi keuangan yang sebelumnya lebih banyak dibatasi oleh rezim kerahasiaan sektoral. Pada level pelaksanaan, PMK Nomor 108 Tahun 2025 diposisikan sebagai regulasi teknis mutakhir yang memperkuat kerangka akses informasi keuangan untuk kepentingan perpajakan, termasuk pembacaan terhadap CRS, Amended CRS, dan CARF.[5]

Perkembangan tersebut harus dibaca bersama dengan lahirnya UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Setelah UU PDP berlaku, pengelolaan data keuangan untuk kepentingan perpajakan tidak cukup dinilai dari ada atau tidaknya kewenangan akses, tetapi juga harus diuji berdasarkan prinsip legalitas, pembatasan tujuan, proporsionalitas, akuntabilitas, keamanan, dan transfer data lintas batas.[6] Prinsip-prinsip tersebut menjadi relevan karena data AEOI dapat mengungkap kondisi finansial, relasi ekonomi, dan potensi kepatuhan pajak orang pribadi maupun badan. Selain itu, implementasi AEOI juga berkaitan dengan rezim sistem elektronik.[7] UU ITE sebagaimana diubah terakhir dengan UU Nomor

[4] Putri Anggia et al., "Legal Implications of FATCA in Indonesia: An Analysis of the Viability of the IGA Model 1C Approach," *Jambura Law Review* 8, no. 1 (2026): 307 – 325, https://www.scopus.com/inward/record.uri?eid=2-s2.0-105042618524&partnerID=40&md5=484513d777ed18aa4ad14e8b0d206116.

[5] Ressita Ramadhani, Zakka Farisy, and Dina Silvia Puteri, "COMPARATIVE ANALYSIS OF CBDC AND TAX LAW ENFORCEMENT IN SELECTED COUNTRIES," *Journal of Central Banking Law and Institutions* 4, no. 1 (2025): 141 – 180, https://doi.org/10.21098/jcli.v4i1.275.

[6] Tegar Islami Putra et al., "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study," *Unnes Law Journal* 10, no. 2 (2024): 232 – 254, https://doi.org/10.15294/ulj.v11i2.8928.

[7] Yudhistira Nugraha, Kautsarina, and Ashwin Sasongko Sastrosubroto, "Towards Data Sovereignty in Cyberspace," in *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015* (Institute of Electrical and Electronics Engineers Inc., 2015), 465 – 471, https://doi.org/10.1109/ICoICT.2015.7231469.

1 Tahun 2024, PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital menunjukkan bahwa negara mempunyai tanggung jawab untuk memastikan sistem elektronik berjalan secara andal, aman, dan dapat dipertanggungjawabkan. AEOI menempatkan data perpajakan dalam arus digital lintas batas sehingga keamanan informasi menjadi bagian yang tidak terpisahkan dari legitimasi pertukaran data.

Dari perspektif kedaulatan siber, persoalan utama bukan hanya apakah Indonesia berhak mengirim dan menerima data melalui AEOI, melainkan apakah negara tetap memiliki kendali normatif atas data strategis yang berasal dari yurisdiksinya.[8] Kedaulatan siber menuntut kemampuan negara untuk mengatur arus data, menentukan batas penggunaan, menetapkan standar keamanan, dan memastikan pertanggungjawaban ketika terjadi penyalahgunaan atau kegagalan perlindungan.[9] Dalam konteks ini, AEOI menjadi arena pengujian kemampuan negara untuk menyeimbangkan transparansi fiskal global dengan perlindungan data pribadi dan keamanan informasi perpajakan. Berdasarkan uraian tersebut, artikel ini mengajukan dua pertanyaan hukum. Pertama, bagaimana konstruksi pengaturan AEOI-CRS dan AEOI-CARF di Indonesia dalam kaitannya dengan kedaulatan siber dan tanggung jawab negara melindungi data keuangan perpajakan? Kedua, bagaimana kesesuaian pengaturan tersebut dengan prinsip pelindungan data pribadi dan norma digitalisasi sistem elektronik dalam hukum Indonesia? Jawaban atas pertanyaan tersebut diperlukan untuk menunjukkan apakah pengaturan AEOI telah memadai secara formal sekaligus substantif.

Penelitian ini menggunakan metode yuridis normatif. Metode ini dipilih karena isu utama yang dikaji berkaitan dengan konstruksi norma, kesesuaian antarrezim hukum, dan kebutuhan penguatan pengaturan.[10] Fokus penelitian bukan pada pengukuran empiris efektivitas kebijakan, melainkan pada penelaahan bahan hukum yang mengatur AEOI, pelindungan data pribadi, sistem elektronik, dan keamanan informasi perpajakan. Pendekatan yang digunakan meliputi pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan terbatas. Pendekatan perundang-undangan digunakan untuk menelaah

[8] Ferry Irawan Febriansyah et al., "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," *International Journal of Law and Society* 5, no. 1 (2026): 26 – 44, https://doi.org/10.59683/ijls.v5i1.357.

[9] Indirwan and Sarah Safira Aulianisa, "Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia," *Lex Scientia Law Review* 4, no. 1 (2020): 30 – 45, https://doi.org/10.15294/lesrev.v4i1.38197.

[10] Yeni Widowaty Sayang Bidul, "ENFORCEMENT OF LAW REGARDING ENVIRONMENTAL DAMAGE DUE TO MINING ACTIVITIES" 23, no. 2 (2024): 1–13.

UU Nomor 9 Tahun 2017, UU KUP beserta perubahan-perubahannya, UU Nomor 27 Tahun 2022, UU ITE sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024, PP Nomor 71 Tahun 2019, Perpres Nomor 82 Tahun 2022, PMK Nomor 108 Tahun 2025, dan PER-10/PJ/2025. Pendekatan konseptual digunakan untuk membaca konsep kedaulatan negara, kedaulatan siber, pelindungan data pribadi, transfer data lintas batas, dan keamanan informasi. Pendekatan perbandingan terbatas digunakan untuk menilai posisi hukum nasional terhadap standar OECD mengenai CRS, Amended CRS, CARF, confidentiality, dan data safeguards.

Bahan hukum primer dalam penelitian ini meliputi peraturan perundang-undangan nasional dan instrumen internasional yang relevan dengan AEOI. Bahan hukum sekunder meliputi buku, artikel jurnal, penelitian terdahulu, serta dokumen akademik mengenai hukum perpajakan internasional, pelindungan data pribadi, dan keamanan siber. Bahan hukum tersier digunakan sepanjang diperlukan untuk menjelaskan istilah hukum dan teknis yang relevan. Analisis dilakukan secara kualitatif melalui penafsiran gramatikal, sistematis, teleologis, dan argumentatif. Penafsiran gramatikal digunakan untuk memahami rumusan norma. Penafsiran sistematis digunakan untuk menghubungkan rezim perpajakan, rezim pelindungan data, dan rezim sistem elektronik. Penafsiran teleologis digunakan untuk membaca tujuan pengaturan, terutama keseimbangan antara transparansi fiskal dan pelindungan hak. Hasil analisis kemudian diarahkan pada dua dimensi, yaitu lex lata untuk menjelaskan hukum yang berlaku dan lex ferenda untuk merumuskan arah penguatan hukum.

B. PEMBAHASAN

B.1 Konstruksi pengaturan AEOI-CRS dan AEOI-CARF di Indonesia

Konstruksi pengaturan AEOI di Indonesia dibangun melalui jaringan norma yang berlapis. Pada lapis pertama terdapat dasar legitimasi berupa UU Nomor 9 Tahun 2017. Undang-undang ini membuka akses informasi keuangan untuk kepentingan perpajakan dan menandai pergeseran dari kerahasiaan sektoral menuju keterbukaan terbatas.[11] Keterbukaan tersebut tidak bersifat bebas, melainkan dibenarkan sepanjang dilakukan untuk tujuan perpajakan dan berdasarkan mekanisme hukum yang telah ditetapkan. Pada lapis kedua terdapat norma administrasi perpajakan yang lebih umum, terutama UU KUP beserta perubahan-perubahannya.[12]

[11] Anggia et al., "Legal Implications of FATCA in Indonesia: An Analysis of the Viability of the IGA Model 1C Approach."
[12] Ramadhani, Farisy, and Puteri, "COMPARATIVE ANALYSIS OF CBDC AND TAX LAW ENFORCEMENT IN SELECTED COUNTRIES."

Norma ini penting karena mengatur kewenangan administrasi perpajakan, penggunaan data, kewajiban pemberian keterangan, dan prinsip kerahasiaan jabatan. Dengan demikian, akses informasi keuangan tidak berdiri sendiri, melainkan menjadi bagian dari rezim administrasi pajak yang memiliki tujuan pengawasan, pemeriksaan, dan penegakan kepatuhan.

Pada lapis ketiga terdapat aturan teknis pelaksanaan. PMK Nomor 108 Tahun 2025 diposisikan sebagai regulasi teknis yang memperbarui tata kelola akses informasi keuangan untuk kepentingan perpajakan. Regulasi ini penting karena ruang lingkup AEOI tidak lagi hanya dibaca sebagai CRS atas informasi rekening keuangan, tetapi juga sebagai Amended CRS dan CARF atas informasi aset kripto relevan. PER-10/PJ/2025 kemudian relevan dalam kerangka pelaksanaan pertukaran informasi berdasarkan perjanjian internasional.[13] Pada lapis keempat terdapat standar internasional, terutama CRS, Amended CRS, CARF MCAA, CRS MCAA, Addendum to the CRS MCAA, dan dokumen OECD mengenai confidentiality serta data safeguards. Standar ini menentukan jenis data yang dipertukarkan, prosedur due diligence, hubungan antarotoritas, dan ukuran pengamanan informasi. Dengan demikian, hukum nasional tidak hanya berfungsi memberi legitimasi internal, tetapi juga harus kompatibel dengan standar global agar pertukaran informasi dapat berjalan efektif.[14]

Perbandingan antara CRS, Amended CRS, dan CARF menunjukkan bahwa perluasan AEOI membawa konsekuensi hukum yang semakin kompleks. CRS terutama berhubungan dengan informasi rekening keuangan. Amended CRS memperluas penyesuaian terhadap perkembangan produk keuangan digital.[15] CARF bergerak lebih jauh dengan menempatkan transaksi aset kripto relevan sebagai objek pelaporan dan pertukaran otomatis. Perbedaan objek tersebut berimplikasi pada jenis data, aktor pelapor, risiko keamanan, dan kebutuhan pelindungan data.

Tabel 1

Perbandingan CRS, Amended CRS, dan CARF

[13] Sidik Prabowo et al., "Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia," *International Journal of Safety and Security Engineering* 15, no. 1 (2025): 113 – 126, https://doi.org/10.18280/ijsse.150113.

[14] Denindah Olivia, "Legal Aspects of Artificial Intelligence on Automated Decision-Making in Indonesia: Lessons from the European Union, the United States, and China," *Lentera Hukum* 7, no. 3 (2020): 301 – 318, https://doi.org/10.19184/ejlh.v7i3.18380.

[15] Upik Mutiara et al., "Exceptions of Banking Secrets for The Interest of Taxes in Indonesia (a Comparation of The Post-Birth of Access Law to Financial Information)," *Legality: Jurnal Ilmiah Hukum* 28, no. 2 (2020): 196 – 210, https://doi.org/10.22219/ljih.v28i2.13375.

Aspek	CRS	Amended CRS	CARF
Objek utama	Informasi rekening keuangan yang dilaporkan oleh lembaga keuangan pelapor.	Perluasan CRS terhadap produk keuangan digital tertentu dan instrumen yang berhubungan dengan aset kripto.	Informasi aset kripto relevan dan transaksi yang dilaporkan oleh penyedia jasa atau entitas yang memenuhi kriteria CARF.
Fokus due diligence	Identifikasi pemegang rekening dan pihak pengendali yang relevan untuk tujuan perpajakan.	Penguatan prosedur identifikasi dan rincian pelaporan sesuai perkembangan produk keuangan digital.	Identifikasi pengguna aset kripto, pihak pengendali, yurisdiksi pajak, dan transaksi aset kripto yang masuk ruang pelaporan.
Implikasi pelindungan data	Risiko utama pada identitas, saldo, penghasilan, dan kerahasiaan rekening.	Risiko bertambah karena cakupan data meluas ke produk digital.	Risiko lebih kompleks karena data berkaitan dengan transaksi digital, penyedia jasa, dan perpindahan nilai lintas yurisdiksi.
Implikasi kedaulatan siber	Negara perlu menjaga kendali normatif atas data keuangan lintas batas.	Negara perlu menyesuaikan safeguard terhadap produk digital yang masuk lingkup CRS.	Negara perlu memperkuat kontrol atas data perpajakan digital dan ekosistem aset kripto lintas batas.

Perluasan dari CRS menuju CARF memperlihatkan bahwa AEOI tidak lagi cukup dipahami sebagai mekanisme pelaporan rekening keuangan. CARF membawa karakter data yang lebih digital, lebih cepat berpindah lintas yurisdiksi, dan berpotensi melibatkan aktor yang tidak selalu sama dengan lembaga keuangan tradisional. Karena itu, penguatan hukum tidak hanya diperlukan pada aspek akses informasi, tetapi juga pada klasifikasi data, kontrol penggunaan, penelusuran akses, dan standar keamanan sistem elektronik.

B.2 AEOI, kedaulatan siber, dan tanggung jawab negara atas data strategis

Kedaulatan negara dalam hukum modern tidak dapat lagi dipahami hanya sebagai kewenangan absolut dalam wilayah fisik. Perkembangan ruang digital melahirkan kebutuhan untuk membaca kedaulatan melalui kemampuan negara mengatur sistem elektronik, infrastruktur digital, dan

arus data yang berdampak terhadap kepentingan nasional.[16] Dalam konteks ini, kedaulatan siber menjadi konsep penting untuk menilai bagaimana negara menjalankan otoritasnya atas data strategis yang bergerak lintas batas.[17] AEOI mempertemukan dua kepentingan yang sama-sama penting. Di satu sisi, negara memerlukan akses informasi untuk menegakkan hukum pajak dan menutup ruang penghindaran pajak. Di sisi lain, data yang dipertukarkan merupakan data sensitif yang dapat menggambarkan identitas, posisi finansial, struktur kekayaan, dan pola hubungan ekonomi lintas yurisdiksi. Karena itu, data AEOI tidak dapat diposisikan sebagai data administratif biasa, melainkan sebagai data strategis perpajakan yang memerlukan perlindungan khusus.[18]

Partisipasi Indonesia dalam AEOI tidak dapat serta-merta dipandang sebagai pelemahan kedaulatan. Sebaliknya, keterlibatan tersebut dapat dibaca sebagai bentuk kedaulatan adaptif karena negara secara sadar memilih masuk ke rezim transparansi global untuk memperkuat kepentingan fiskalnya. Kedaulatan tidak diukur dari tertutup atau terbukanya data, tetapi dari kemampuan negara menentukan dasar hukum, batas penggunaan, standar perlindungan, dan pertanggungjawaban atas data yang dipertukarkan.[19] Masalah hukum muncul ketika perluasan akses dan pertukaran data bergerak lebih cepat daripada penguatan safeguard domestik. AEOI membuka kemungkinan satu data digunakan oleh berbagai unit pengawasan dalam rentang waktu yang berbeda. Apabila pemanfaatan ulang data tidak didukung audit trail, pembatasan tujuan, dan pengendalian akses yang tegas, maka risiko function creep meningkat. Function creep dalam konteks ini berarti perluasan fungsi data di luar batas yang secara jelas dirumuskan pada saat data dikumpulkan atau dipertukarkan.[20]

---

[16] Anija Nazrul and Nazrul Islam, *Interglobal Competition and Digital Sovereignty: How Firms Build Agility Across Borders*, *DigiTech Agility for Business Competitiveness and Innovation Imperatives* (IGI Global, 2026), https://doi.org/10.4018/979-8-3373-4601-4.ch003.

[17] Melike Melis Dilisen, "Sovereignty over Cyber Territories," *International Journal of Interdisciplinary Civic and Political Studies* 13, no. 3–4 (2018): 1 – 11, https://doi.org/10.18848/2327-0071/CGP/v13i02/1-11.

[18] Tatyana V Karlova, Alexander Y Bekmeshov, and Natalia M Kuznetsova, "Protection the Data Banks in State Critical Information Infrastructure Organizations," in *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019*, ed. Shaposhnikov S.O. and Saint Petersburg Saint Petersburg Electrotechnical University "LETI" Popov Str. 5 (Institute of Electrical and Electronics Engineers Inc., 2019), 155 – 157, https://doi.org/10.1109/ITQMIS.2019.8928412.

[19] Abdulqadous Abdullah et al., "Sovereignty in the Digital Age: Social, Legal, and Governance Challenges of Global Networks," ed. Molamohamadi Z. et al., *Communications in Computer and Information Science* 2855 CCIS (2026): 143 – 159, https://doi.org/10.1007/978-3-032-17023-1_8.

[20] Loriana Crasnic and Lukas Hakelberg, *Power and Resistance in the Global Fight against Tax Evasion*, *Handbook on the Politics of Taxation* (Edward Elgar Publishing Ltd., 2021), https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126953254&partnerID=40&md5=a5822f9655d5fe6062695928e4616e29.

Tanggung jawab negara dalam AEOI tidak berhenti pada pembentukan dasar hukum akses informasi. Negara juga harus memastikan bahwa data tidak dicuri, diambil, diakses, digunakan ulang, atau dialihkan oleh pihak yang tidak berwenang.[21] Tanggung jawab ini meliputi pembentukan norma yang jelas, pengamanan sistem elektronik, mekanisme kontrol akses, pencatatan jejak pemanfaatan data, respons insiden, dan konsekuensi hukum apabila terjadi kegagalan pelindungan. Dengan demikian, kedaulatan siber dalam AEOI bekerja melalui kontrol normatif dan institusional atas seluruh siklus pemrosesan data.

B.3 Kesesuaian AEOI dengan prinsip pelindungan data pribadi

Dalam UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi parameter penting dalam menilai legalitas dan kelayakan pemrosesan data AEOI. Data keuangan yang dipertukarkan dalam AEOI dapat termasuk data pribadi yang sensitif karena memuat informasi mengenai kondisi finansial subjek data. Karena itu, akses dan pertukaran data harus diuji berdasarkan prinsip legalitas, pembatasan tujuan, proporsionalitas, minimisasi data, akuntabilitas, keamanan, dan transfer data lintas batas.[22] Dari sisi legalitas, implementasi AEOI di Indonesia memiliki dasar hukum yang memadai. UU Nomor 9 Tahun 2017 memberikan legitimasi bagi akses informasi keuangan untuk kepentingan perpajakan, sedangkan regulasi teknis mengatur tata cara pelaporan dan pertukaran data. Legalitas ini penting karena pemrosesan data untuk kepentingan perpajakan pada umumnya bertumpu pada kewenangan hukum publik, bukan pada persetujuan subjek data.[23]

Meskipun legalitas awal terpenuhi, legalitas tidak otomatis menyelesaikan seluruh persoalan perlindungan data. Prinsip pembatasan tujuan menuntut agar data AEOI hanya digunakan untuk kepentingan perpajakan sesuai tujuan pengumpulannya. Dalam hal data digunakan berulang untuk kepentingan pengawasan, perlu ada mekanisme pencatatan yang menunjukkan siapa yang mengakses, untuk tujuan apa, pada waktu kapan, dan berdasarkan dasar kewenangan apa. Tanpa mekanisme tersebut, pembatasan tujuan akan sulit diawasi secara

---

[21] Atilla Aydin and Turksel Kaya Bensghir, "Digital Data Sovereignty: Towards a Conceptual Framework," in *1st International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation, IISEC 2019 - Proceedings*, ed. Varol A. et al. (Institute of Electrical and Electronics Engineers Inc., 2019), https://doi.org/10.1109/UBMYK48245.2019.8965469.

[22] Stjepan Gadžo and Irena Klemenčić, "Effective International Information Exchange as a Key Element of Modern Tax Systems: Promises and Pitfalls of the OECD's Common Reporting Standard," *Public Sector Economics* 41, no. 2 (2017): 207 – 226, https://doi.org/10.3326/pse.41.2.3.

[23] Rizky Amalia Kurnia, Dhata Praditya, and Marijn Janssen, "A Comparative Study of Business-to-Government Information Sharing Arrangements for Tax Reporting," ed. Dwivedi Y. et al., *IFIP Advances in Information and Communication Technology* 558 (2019): 154 – 169, https://doi.org/10.1007/978-3-030-20671-0_11.

efektif.[24] Dari sisi proporsionalitas dan minimisasi data, rezim AEOI memang memerlukan pengumpulan informasi yang cukup luas agar pertukaran dapat efektif. Namun, keluasan tersebut tetap harus diuji terhadap kebutuhan yang sah. Data yang dikumpulkan seharusnya tidak melampaui informasi yang relevan untuk tujuan perpajakan. Dalam konteks CARF, pengujian proporsionalitas menjadi semakin penting karena data aset kripto dapat meliputi informasi transaksi digital, identitas pengguna, pihak pengendali, dan penyedia jasa yang terkait.[25]

Dari sisi transfer data lintas batas, AEOI menimbulkan risiko khusus karena data bergerak keluar dari wilayah kendali domestik yang paling langsung. UU PDP menuntut agar transfer ke luar wilayah Indonesia memperhatikan dasar hukum dan kecukupan pelindungan. Dalam AEOI, dasar transfer dapat ditopang oleh kewajiban hukum dan perjanjian internasional, tetapi kecukupan pelindungan setelah data diterima yurisdiksi lain tetap memerlukan penegasan melalui safeguard, pengawasan, dan mekanisme penanganan insiden.[26] Dari sisi akuntabilitas, pemrosesan AEOI melibatkan banyak aktor, mulai dari lembaga keuangan pelapor, penyedia jasa aset kripto atau entitas pelapor CARF, otoritas pajak domestik, penyelenggara sistem elektronik, hingga otoritas penerima di luar negeri. Keterlibatan banyak aktor menimbulkan kebutuhan untuk menegaskan siapa yang bertindak sebagai pengendali data, siapa yang menjadi prosesor, bagaimana pembagian tanggung jawab, dan bagaimana konsekuensi hukum apabila terjadi kebocoran atau penyalahgunaan data.[27]

Berdasarkan pengujian tersebut, implementasi AEOI di Indonesia dapat dikatakan sesuai secara formal dengan prinsip perlindungan data pribadi karena memiliki dasar hukum dan tujuan perpajakan yang sah.[28] Namun, kesesuaian tersebut belum optimal secara substantif karena

---

[24] Ahmad Budi Setiawan and Ashwin Sasongko Sastrosubroto, "Strengthening the Security of Critical Data in Cyberspace, a Policy Review," in *Proceeding - 2016 International Conference on Computer, Control, Informatics and Its Applications: Recent Progress in Computer, Control, and Informatics for Data Science, IC3INA 2016* (Institute of Electrical and Electronics Engineers Inc., 2017), 185 – 190, https://doi.org/10.1109/IC3INA.2016.7863047.

[25] Roberto Ramos Obando and Pablo Porporatto, "Taxpayer Rights in the Context of the Automatic Exchange of Information (AEOI): Insights from Recent Swiss Case Law," *European Taxation* 65, no. 11 (2025): 471 – 478, https://doi.org/10.59403/2seadra.

[26] Elisa Sorrentino et al., "Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive Landscape," in *Proceedings - 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design, IOLTS 2025* (Institute of Electrical and Electronics Engineers Inc., 2025), https://doi.org/10.1109/IOLTS65288.2025.11116851.

[27] André Barrinha and G Christou, "Speaking Sovereignty: The EU in the Cyber Domain," *European Security* 31, no. 3 (2022): 356 – 376, https://doi.org/10.1080/09662839.2022.2102895.

[28] Hisham Eslam and Garima Tiwari, "Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty," *Studies in Computational Intelligence* 1181 (2025): 93 – 112, https://doi.org/10.1007/978-3-031-80557-8_4.

masih diperlukan pengaturan lebih tegas mengenai pembatasan pemanfaatan ulang data, retensi data, standar transfer lintas batas, audit trail, kontrol akses, dan pembagian tanggung jawab hukum.

B.4 Norma sistem elektronik, keamanan informasi, dan kebutuhan safeguard nasional

AEOI dijalankan melalui sistem elektronik yang mengumpulkan, menyimpan, memverifikasi, dan mempertukarkan data lintas yurisdiksi. Oleh karena itu, keamanan informasi menjadi unsur utama dalam menilai kelayakan AEOI.[29] Keamanan informasi dalam konteks ini meliputi kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan memastikan data hanya diakses oleh pihak berwenang. Integritas memastikan data tidak diubah secara tidak sah. Ketersediaan memastikan data dapat digunakan oleh otoritas yang berwenang ketika diperlukan.[30] Hukum nasional telah menyediakan kerangka umum mengenai sistem elektronik. UU ITE dan PP PSTE mengatur kewajiban penyelenggara sistem elektronik untuk menyelenggarakan sistem secara andal, aman, dan bertanggung jawab. Perpres Nomor 82 Tahun 2022 memperkuat perspektif pelindungan infrastruktur informasi vital. UU PDP menambahkan kewajiban pengamanan data pribadi. Secara umum, kerangka ini menunjukkan bahwa AEOI tidak berada dalam kekosongan hukum.[31]

Namun, apabila dibaca khusus terhadap kebutuhan AEOI, norma yang tersedia masih bersifat umum. Rezim perpajakan lebih kuat mengatur akses, pelaporan, dan pertukaran informasi, sedangkan rezim sistem elektronik lebih kuat mengatur keandalan dan keamanan sistem secara umum. Celah normatif terletak pada belum adanya desain safeguard nasional yang secara spesifik menghubungkan keduanya untuk data AEOI-CRS dan AEOI-CARF.[32] Standar OECD mengenai confidentiality dan data safeguards menunjukkan bahwa pertukaran informasi otomatis

[29] Xiaoqing Huang, "Ensuring Taxpayer Rights in the Era of Automatic Exchange of Information: EU Data Protection Rules and Cases," *Intertax* 46, no. 3 (2018): 225 – 239, https://doi.org/10.54648/taxi2018024.
[30] Mahmoud Ismail et al., "Conceptual and Legal Issues for National Cyber Sovereignty," ed. Alzoubi H.M., Al-Gasaymeh A.S., and Vasudevan S., *Advances in Science, Technology and Innovation*, 2025, 197 – 201, https://doi.org/10.1007/978-3-031-90558-2_25.
[31] Ahmad Aqeil Alzaqibh and Husein Bani Issa, "Digital Sovereignty and Data Localization in International Legal Systems: Trying to Balance State Control and the Global Digital Economy," in *2026 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2026* (Institute of Electrical and Electronics Engineers Inc., 2026), 778 – 783, https://doi.org/10.1109/ICETSIS68266.2026.11549231.
[32] Sri Mulyani, Suparno Suparno, and Retno Mawarini Sukmariningsih, "Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy," *International Journal of Cyber Criminology* 17, no. 2 (2023): 133 – 146, https://doi.org/10.5281/zenodo.4766709.

mensyaratkan pengamanan yang kuat.[33] Standar tersebut tidak hanya menuntut kewajiban menjaga kerahasiaan, tetapi juga kebijakan keamanan, kontrol akses, manajemen risiko, pelatihan, pengelolaan insiden, audit, dan akuntabilitas.[34] Oleh karena itu, kecukupan pengaturan nasional perlu dinilai bukan hanya dari keberadaan norma umum, tetapi juga dari kemampuannya memenuhi standar operasional pengamanan data yang nyata.

Tabel 2

Peta Rezim Keamanan Informasi yang Relevan bagi AEOI

Rezim	Sumber Norma	Kekuatan	Kelemahan/Relevansi
Sistem elektronik	UU ITE, PP 71/2019, Perpres 82/2022	Memberi dasar keandalan, keamanan, audit, dan manajemen risiko sistem elektronik.	Masih bersifat umum dan belum secara khusus mengatur karakter data AEOI-CRS dan AEOI-CARF.
Pelindungan data pribadi	UU 27/2022	Menegaskan prinsip legalitas, pembatasan tujuan, keamanan pemrosesan, dan transfer data lintas batas.	Belum sepenuhnya diterjemahkan ke dalam tata kelola sektoral perpajakan dan AEOI-CARF.
Perpajakan dan AEOI	UU 9/2017, UU KUP, PMK 108/2025, PER-10/PJ/2025	Memberi legitimasi langsung bagi akses, pelaporan, dan pertukaran data.	Lebih kuat pada pembukaan akses daripada standar keamanan spesifik dan pertanggungjawaban lintas aktor.
Standar internasional	CRS, Amended CRS, CARF MCAA, dokumen OECD data safeguards	Memberi ukuran eksternal mengenai confidentiality, safeguard, due diligence, dan pertukaran data.	Perlu diterjemahkan secara tegas ke dalam hukum nasional agar tidak berhenti pada kepatuhan formal.

Peta tersebut menunjukkan bahwa persoalan utama bukan ketiadaan norma, melainkan keterpaduan norma. Setiap rezim menyediakan unsur perlindungan tertentu, tetapi belum seluruhnya disatukan dalam satu desain operasional yang secara khusus ditujukan

[33] Segundo Moisés T Toapanta, Marjorie Isanoa Sinche, and Luis Enrique Mafla Gallegos, "A Cyber Environment Approach to Mitigate Vulnerabilities and Threats in an Electoral Process in Ecuador," in *ACM International Conference Proceeding Series* (Association for Computing Machinery, 2019), 97 – 104, https://doi.org/10.1145/3375900.3375914.

[34] Elaine Hulitt and Rayford B Vaughn Jr., "Information System Security Compliance to FISMA Standard: A Quantitative Measure," in *Proceedings of the International Multiconference on Computer Science and Information Technology, IMCSIT 2008*, vol. 3, 2008, 799 – 806, https://doi.org/10.1109/IMCSIT.2008.4747334.

bagi data AEOI.[35] Ketika data dipertukarkan lintas yurisdiksi, keterpaduan menjadi penting karena insiden dapat terjadi pada tahap pengumpulan, penyimpanan, transmisi, penggunaan domestik, atau setelah data diterima oleh yurisdiksi mitra. Karena itu, safeguard nasional perlu dirumuskan sebagai jembatan antara hukum perpajakan, hukum perlindungan data, dan hukum sistem elektronik.[36] Safeguard tersebut sebaiknya memuat klasifikasi data AEOI sebagai data sensitif, kontrol akses berbasis kewenangan, pembatasan pemanfaatan ulang, audit trail, standar enkripsi dan keamanan transmisi, retensi data, audit berkala, pelatihan petugas, serta prosedur respons insiden. Tanpa jembatan tersebut, pengaturan AEOI berisiko kuat secara administratif tetapi lemah dari sisi pelindungan operasional.

B.5 Arah penguatan hukum AEOI di Indonesia

Arah penguatan hukum AEOI perlu ditempatkan pada tujuan menjaga keseimbangan antara transparansi fiskal global dan perlindungan hak. Transparansi fiskal merupakan tujuan yang sah dan penting, tetapi tidak boleh berkembang menjadi perluasan akses yang tidak terkendali.[37] Pelindungan data pribadi juga penting, tetapi tidak dapat dipahami sebagai penghalang mutlak terhadap kepentingan perpajakan. Keduanya harus ditempatkan dalam desain hukum yang memastikan kewenangan negara berjalan dengan batas, pengawasan, dan pertanggungjawaban.[38]

Pertama, harmonisasi antara rezim perpajakan, UU PDP, dan rezim sistem elektronik perlu diperkuat. Harmonisasi ini tidak cukup dilakukan melalui pernyataan umum bahwa data harus dilindungi. Diperlukan penjabaran yang lebih konkret mengenai hubungan antara dasar pemrosesan data dalam perpajakan dengan prinsip pengendalian data

[35] Syifaurachman and Antoni Wibowo, "RISK ASSESSMENT RELATED TO PRIVACY INFORMATION ON ELECTRONIC MONEY SERVER-BASED USING ISO 27001 ISO 27005, ISO 27701," *Journal of Theoretical and Applied Information Technology* 101, no. 3 (2023): 1067 – 1077, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85153800017&partnerID=40&md5=98ca981f35cdafb7790e4b1d8f8ef5fe.

[36] Yasuyuki Kawanishi et al., "Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002," ed. Bitsch F., Tonetta S., and Schoitsch E., *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10489 LNCS (2017): 211 – 224, https://doi.org/10.1007/978-3-319-66284-8_18.

[37] Vasiliki Diamantopoulou, Aggeliki Tsohou, and Maria Karyda, "From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance," ed. Katsikas S. et al., *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11980 LNCS (2020): 238 – 257, https://doi.org/10.1007/978-3-030-42048-2_16.

[38] Rasim Alguliyev, Yadigar Imamverdiyev, and Elchin Aliyev, "Conceptual Architecture of National Information Space Security System of Azerbaijan," in *2012 4th International Conference "Problems of Cybernetics and Informatics", PCI 2012 - Proceedings*, 2012, https://doi.org/10.1109/ICPCI.2012.6486262.

dalam UU PDP, termasuk posisi pengendali data, prosesor data, dan pihak yang memiliki akses terhadap data AEOI.

Kedua, perlu penegasan pembatasan tujuan dan pemanfaatan ulang data. Data AEOI seharusnya hanya digunakan untuk kepentingan perpajakan yang sah. Setiap penggunaan ulang perlu memiliki dasar kewenangan, tujuan yang dapat ditelusuri, dan catatan akses yang dapat diaudit. Hal ini penting untuk mencegah function creep dan memastikan data tidak digunakan secara berlebihan atau tidak proporsional.

Ketiga, standar keamanan informasi AEOI perlu dibuat lebih spesifik. Standar tersebut perlu mencakup klasifikasi data, pembatasan akses, enkripsi, pengujian keamanan, audit berkala, manajemen risiko, dan respons insiden. Untuk AEOI-CARF, standar tersebut harus menyesuaikan karakter aset kripto yang digital, lintas batas, dan melibatkan penyedia jasa atau entitas pelapor yang berbeda dari lembaga keuangan tradisional.

Keempat, perlu pembagian tanggung jawab lintas aktor. Lembaga pelapor bertanggung jawab atas akurasi dan keamanan data sebelum disampaikan. Otoritas pajak bertanggung jawab atas pengelolaan, penggunaan, dan pertukaran data. Penyelenggara sistem elektronik bertanggung jawab atas keandalan dan keamanan sistem. Mitra yurisdiksi penerima harus tunduk pada komitmen confidentiality dan data safeguards. Pembagian ini perlu dirumuskan agar insiden tidak berhenti pada saling lempar tanggung jawab.

Kelima, perlu penguatan mekanisme audit trail. Audit trail tidak hanya berguna untuk kepentingan teknis, tetapi juga menjadi instrumen akuntabilitas hukum.[39] Melalui audit trail, dapat ditelusuri siapa yang mengakses data, kapan akses dilakukan, untuk kepentingan apa, dan apakah akses tersebut sesuai dengan kewenangan yang diberikan. Dalam konteks data AEOI, audit trail menjadi syarat penting untuk menjaga kedaulatan siber karena negara dapat mempertahankan kendali normatif atas data strategis yang dikelolanya.[40]

Tabel 3

Agenda Penguatan Hukum AEOI di Indonesia

Isu	Celah Utama	Arah Penguatan

[39] Hulitt and Vaughn Jr., "Information System Security Compliance to FISMA Standard: A Quantitative Measure."

[40] Rishita Masiwal et al., *Balancing Technology and Trust: The Impact of Health Information Technology on Data Security and Patient Confidence in Healthcare*, *Quantum Learning: Bridging Artificial Intelligence, Quantum Computing, and Data Science in Education* (CRC Press, 2026), https://doi.org/10.1201/9781003637400-16.

Pembatasan tujuan	Belum cukup tegas mengatur pemanfaatan ulang data AEOI.	Tetapkan batas penggunaan, dasar akses ulang, dan audit trail pemanfaatan data.
Transfer lintas batas	Kecukupan pelindungan setelah data diterima yurisdiksi lain belum rinci.	Perkuat safeguard, evaluasi yurisdiksi penerima, dan mekanisme penanganan insiden lintas yurisdiksi.
AEOI-CARF	Karakter data aset kripto lebih digital, lintas batas, dan melibatkan aktor baru.	Buat standar pengamanan khusus bagi pelaporan dan pertukaran data CARF.
Akuntabilitas	Pembagian tanggung jawab antaraktor belum terintegrasi.	Tegaskan tanggung jawab lembaga pelapor, DJP, PSE, dan mitra penerima.
Keamanan sistem	Norma keamanan masih umum dan tersebar.	Tetapkan standar khusus mengenai kontrol akses, enkripsi, pengujian keamanan, audit, dan respons insiden.

Dengan agenda tersebut, penguatan AEOI tidak diarahkan untuk melemahkan transparansi perpajakan, tetapi untuk membuat transparansi tersebut memiliki legitimasi yang lebih kuat.[41] AEOI akan lebih dapat diterima apabila negara tidak hanya mampu mengakses dan mempertukarkan data, tetapi juga mampu menunjukkan bahwa data tersebut dibatasi penggunaannya, aman secara sistem, dapat diaudit, dan memiliki rantai pertanggungjawaban yang jelas.

C. PENUTUP

Konstruksi pengaturan AEOI di Indonesia telah memiliki dasar legitimasi yang memadai melalui UU Nomor 9 Tahun 2017, UU KUP, PMK Nomor 108 Tahun 2025, PER-10/PJ/2025, dan instrumen internasional terkait CRS, Amended CRS, serta CARF. Partisipasi Indonesia dalam AEOI tidak menghapus kedaulatan negara, melainkan menunjukkan bentuk kedaulatan yang adaptif dalam tata kelola perpajakan global. Namun, kedaulatan tersebut hanya dapat dipertahankan secara substantif apabila negara memiliki kendali normatif atas dasar hukum, batas penggunaan, standar keamanan, dan pertanggungjawaban data yang dipertukarkan. Pengaturan AEOI di Indonesia telah sesuai secara formal dengan prinsip pelindungan data pribadi karena memiliki dasar hukum dan tujuan perpajakan yang sah. Akan tetapi, kesesuaian formal tersebut belum sepenuhnya optimal secara substantif. Titik yang masih memerlukan penguatan meliputi pembatasan tujuan, proporsionalitas pemrosesan, transfer data lintas batas, retensi data, kontrol akses, audit trail,

[41] Siti Mariyam et al., "Safeguarding Personal Data in Indonesian E-Commerce from A Constitutional Rights Perspective," *Jambe Law Journal* 8, no. 2 (2025): 683 – 711, https://doi.org/10.22437/jlj.8.2.683-711.

pemberitahuan insiden, dan pembagian tanggung jawab hukum antaraktor.

Perluasan AEOI melalui CARF memperbesar kebutuhan harmonisasi antara rezim perpajakan, pelindungan data pribadi, dan sistem elektronik. Rezim perpajakan cenderung lebih kuat mengatur akses dan pelaporan, sedangkan rezim sistem elektronik dan pelindungan data menyediakan standar pengamanan yang masih perlu diterjemahkan secara spesifik ke dalam konteks AEOI. Karena itu, penguatan hukum perlu diarahkan pada pembentukan safeguard nasional yang menghubungkan transparansi fiskal, pelindungan data pribadi, keamanan informasi, dan kedaulatan siber.

Artikel ini merekomendasikan harmonisasi norma, penyusunan standar keamanan informasi khusus bagi data AEOI-CRS dan AEOI-CARF, penguatan audit trail, pembatasan pemanfaatan ulang data, serta penegasan tanggung jawab lembaga pelapor, otoritas pajak, penyelenggara sistem elektronik, dan mitra yurisdiksi penerima. Dengan penguatan tersebut, AEOI dapat mendukung kepatuhan perpajakan global tanpa mengurangi pelindungan data pribadi dan kendali hukum negara atas data strategis.

DAFTAR PUSTAKA

Abdullah, Abdulqadous, Suzan Mohammed Jawad Alkazraji, Ayah Ahmed Jasim, Aseel Ibraheem Muhsin, Faris Abdul Kareem Khazal, and Radomyr Mykolenko. “Sovereignty in the Digital Age: Social, Legal, and Governance Challenges of Global Networks.” Edited by Molamohamadi Z., Mirzazadeh A., Babaee Tirkolaee E., and Weber G.-W. *Communications in Computer and Information Science* 2855 CCIS (2026): 143 – 159. https://doi.org/10.1007/978-3-032-17023-1_8.

Alguliyev, Rasim, Yadigar Imamverdiyev, and Elchin Aliyev. “Conceptual Architecture of National Information Space Security System of Azerbaijan.” In *2012 4th International Conference “Problems of Cybernetics and Informatics”, PCI 2012 - Proceedings*, 2012. https://doi.org/10.1109/ICPCI.2012.6486262.

Alzaqibh, Ahmad Aqeil, and Husein Bani Issa. “Digital Sovereignty and Data Localization in International Legal Systems: Trying to Balance State Control and the Global Digital Economy.” In *2026 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2026*, 778 – 783. Institute of Electrical and Electronics Engineers Inc., 2026. https://doi.org/10.1109/ICETSIS68266.2026.11549231.

Aulia, E. (2024). Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dari perspektif kepastian hukum. *UNES Law Review*, 7(1), 220-227.

https://doi.org/10.31933/unesrev.v7i1.2267

Anggia, Putri, Aisyah Ajeng Putri Riyanto, Ani Yunita, and Wuku Astuti. "Legal Implications of FATCA in Indonesia: An Analysis of the Viability of the IGA Model 1C Approach." *Jambura Law Review* 8, no. 1 (2026): 307 – 325. https://www.scopus.com/inward/record.uri?eid=2-s2.0-105042618524&partnerID=40&md5=484513d777ed18aa4ad14e8b0d206116.

Anggia, Putri, Ani Yunita, and Fadia Fitriyanti. "Legal Justice: The Abolition of the Principle of Bank Secrecy for Tax Interests in Indonesia." *Jambura Law Review* 5, no. 2 (2023): 314 – 331. https://doi.org/10.33756/jlr.v5i2.18793.

Aydin, Atilla, and Turksel Kaya Bensghir. "Digital Data Sovereignty: Towards a Conceptual Framework." In *1st International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation, IISEC 2019 - Proceedings*, edited by Varol A., Yazici A., Yazici M.A., Varol C., Aygunes G.S., and Cotur A. Institute of Electrical and Electronics Engineers Inc., 2019. https://doi.org/10.1109/UBMYK48245.2019.8965469.

Barrinha, André, and G Christou. "Speaking Sovereignty: The EU in the Cyber Domain." *European Security* 31, no. 3 (2022): 356 – 376. https://doi.org/10.1080/09662839.2022.2102895.

Bhakti, Agus, Arfin Sudirman, R Widya Setiabudi Sumadinata, and Arry Bainus. "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia." *Journal of Human Security* 20, no. 1 (2024): 109 – 117. https://doi.org/10.12924/johs2024.20116.

Crasnic, Loriana, and Lukas Hakelberg. *Power and Resistance in the Global Fight against Tax Evasion. Handbook on the Politics of Taxation*. Edward Elgar Publishing Ltd., 2021. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126953254&partnerID=40&md5=a5822f9655d5fe6062695928e4616e29.

Darmanti, R. M., & Mangkan, D. (2020). The implementation of Automatic Exchange of Information as a tool to tackle offshore tax evasion: An experience from Indonesia. *Scientax: Jurnal Kajian Ilmiah Perpajakan Indonesia*, 2(1), 100-122. https://doi.org/10.52869/st.v2i1.61

Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. "From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance." Edited by Katsikas S., Katsikas S., Cuppens F., Cuppens N., Lambrinoudakis C., Gritzalis S., Kalloniatis C., et al. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11980 LNCS (2020): 238 – 257. https://doi.org/10.1007/978-3-030-42048-2_16.

Dilisen, Melike Melis. "Sovereignty over Cyber Territories." *International Journal of Interdisciplinary Civic and Political Studies* 13, no. 3–4 (2018): 1 – 11. https://doi.org/10.18848/2327-0071/CGP/v13i02/1-11.

Eslam, Hisham, and Garima Tiwari. "Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty." *Studies in Computational Intelligence* 1181 (2025): 93 – 112. https://doi.org/10.1007/978-3-031-80557-8_4.

Febriansyah, Ferry Irawan, Afiful Ikhwan, Ulya Shafa Firdausi, and Ayub Dwi Anggoro. "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity." *International Journal of Law and Society* 5, no. 1 (2026): 26 – 44. https://doi.org/10.59683/ijls.v5i1.357.

Gadžo, Stjepan, and Irena Klemenčić. "Effective International Information Exchange as a Key Element of Modern Tax Systems: Promises and Pitfalls of the OECD's Common Reporting Standard." *Public Sector Economics* 41, no. 2 (2017): 207 – 226. https://doi.org/10.3326/pse.41.2.3.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1), 1-17. https://doi.org/10.1177/2053951720982012

Halim, I. R. (2021). *Analisis penegakan hukum Undang-Undang Nomor 9 Tahun 2017 tentang akses informasi keuangan untuk kepentingan perpajakan terkait data dan informasi perpajakan*. Skripsi, Universitas Gadjah Mada.

Huang, Xiaoqing. "Ensuring Taxpayer Rights in the Era of Automatic Exchange of Information: EU Data Protection Rules and Cases." *Intertax* 46, no. 3 (2018): 225 – 239. https://doi.org/10.54648/taxi2018024.

Hulitt, Elaine, and Rayford B Vaughn Jr. "Information System Security Compliance to FISMA Standard: A Quantitative Measure." In *Proceedings of the International Multiconference on Computer Science and Information Technology, IMCSIT 2008*, 3:799 – 806, 2008. https://doi.org/10.1109/IMCSIT.2008.4747334.

Indirwan, and Sarah Safira Aulianisa. "Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4, no. 1 (2020): 30 – 45. https://doi.org/10.15294/lesrev.v4i1.38197.

Ismail, Mahmoud, Noor Saleh Ali Alzyoud, Fayez A L Nusair, and Randa E L Hasi. "Conceptual and Legal Issues for National Cyber Sovereignty." Edited by Alzoubi H.M., Al-Gasaymeh A.S., and Vasudevan S. *Advances in Science, Technology and Innovation*, 2025, 197 – 201. https://doi.org/10.1007/978-3-031-90558-2_25.

Karlova, Tatyana V, Alexander Y Bekmeshov, and Natalia M Kuznetsova. "Protection the Data Banks in State Critical Information Infrastructure Organizations." In *Proceedings of the 2019 IEEE International*

Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019, edited by Shaposhnikov S.O. and Saint Petersburg Saint Petersburg Electrotechnical University "LETI" Popov Str. 5, 155 – 157. Institute of Electrical and Electronics Engineers Inc., 2019. https://doi.org/10.1109/ITQMIS.2019.8928412.

Kawanishi, Yasuyuki, Hideaki Nishihara, Daisuke Souma, and Hirotaka Yoshida. "Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002." Edited by Bitsch F., Tonetta S., and Schoitsch E. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10489 LNCS (2017): 211 – 224. https://doi.org/10.1007/978-3-319-66284-8_18.

Kurnia, Rizky Amalia, Dhata Praditya, and Marijn Janssen. "A Comparative Study of Business-to-Government Information Sharing Arrangements for Tax Reporting." Edited by Dwivedi Y., Ayaburi E., Boateng R., and Effah J. *IFIP Advances in Information and Communication Technology* 558 (2019): 154 – 169. https://doi.org/10.1007/978-3-030-20671-0_11.

Mariyam, Siti, Adhi Putra Satria, Hariyanto, and Ahmad Masum. "Safeguarding Personal Data in Indonesian E-Commerce from A Constitutional Rights Perspective." *Jambe Law Journal* 8, no. 2 (2025): 683 – 711. https://doi.org/10.22437/jlj.8.2.683-711.

Masiwal, Rishita, Nikita, Deepali Kamthania, and Shailee Bhatia. *Balancing Technology and Trust: The Impact of Health Information Technology on Data Security and Patient Confidence in Healthcare*. *Quantum Learning: Bridging Artificial Intelligence, Quantum Computing, and Data Science in Education*. CRC Press, 2026. https://doi.org/10.1201/9781003637400-16.

Mulyani, Sri, Suparno Suparno, and Retno Mawarini Sukmariningsih. "Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy." *International Journal of Cyber Criminology* 17, no. 2 (2023): 133 – 146. https://doi.org/10.5281/zenodo.4766709.

Mutiara, Upik, Ika Khairunnisa Simanjuntak, Rahmad Ramadhan Hasibuan, and A Amiludin. "Exceptions of Banking Secrets for The Interest of Taxes in Indonesia (a Comparation of The Post-Birth of Access Law to Financial Information)." *Legality: Jurnal Ilmiah Hukum* 28, no. 2 (2020): 196 – 210. https://doi.org/10.22219/ljih.v28i2.13375.

Nazrul, Anija, and Nazrul Islam. *Interglobal Competition and Digital Sovereignty: How Firms Build Agility Across Borders*. *DigiTech Agility for Business Competitiveness and Innovation Imperatives*. IGI Global, 2026. https://doi.org/10.4018/979-8-3373-4601-4.ch003.

Nugraha, Yudhistira, Kautsarina, and Ashwin Sasongko Sastrosubroto.

"Towards Data Sovereignty in Cyberspace." In *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015*, 465 – 471. Institute of Electrical and Electronics Engineers Inc., 2015. https://doi.org/10.1109/ICoICT.2015.7231469.

Obando, Roberto Ramos, and Pablo Porporatto. "Taxpayer Rights in the Context of the Automatic Exchange of Information (AEOI): Insights from Recent Swiss Case Law." *European Taxation* 65, no. 11 (2025): 471 – 478. https://doi.org/10.59403/2seadra.

Olivia, Denindah. "Legal Aspects of Artificial Intelligence on Automated Decision-Making in Indonesia: Lessons from the European Union, the United States, and China." *Lentera Hukum* 7, no. 3 (2020): 301 – 318. https://doi.org/10.19184/ejlh.v7i3.18380.

Pongrekun, Dharma, Arfin Sudirman, Widya Setiabudi, and Arry Bainus. "Digital Sovereignty in the Global South: Indonesia's Cyber Governance between Global Power and National Autonomy." *Research Journal in Advanced Humanities* 7, no. 1 (2026). https://doi.org/10.58256/hprs3b27.

Prabowo, Sidik, Maman Abdurohman, Hilal Hudan Nuha, and Sarwono Sutikno. "Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia." *International Journal of Safety and Security Engineering* 15, no. 1 (2025): 113 – 126. https://doi.org/10.18280/ijsse.150113.

Putra, Tegar Islami, W Waspiah, Indriana Firdaus, Fitria Damayanti, and Bintang Rafli Ananta. "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study." *Unnes Law Journal* 10, no. 2 (2024): 232 – 254. https://doi.org/10.15294/ulj.v11i2.8928.

Ramadhani, Ressita, Zakka Farisy, and Dina Silvia Puteri. "COMPARATIVE ANALYSIS OF CBDC AND TAX LAW ENFORCEMENT IN SELECTED COUNTRIES." *Journal of Central Banking Law and Institutions* 4, no. 1 (2025): 141 – 180. https://doi.org/10.21098/jcli.v4i1.275.

Sayang Bidul, Yeni Widowaty. "Enforcement Of Law Regarding Environmental Damage Due To Mining Activities" 23, no. 2 (2024): 1–13.

Setiawan, Ahmad Budi, and Ashwin Sasongko Sastrosubroto. "Strengthening the Security of Critical Data in Cyberspace, a Policy Review." In *Proceeding - 2016 International Conference on Computer, Control, Informatics and Its Applications: Recent Progress in Computer, Control, and Informatics for Data Science, IC3INA 2016*, 185 – 190. Institute of Electrical and Electronics Engineers Inc., 2017. https://doi.org/10.1109/IC3INA.2016.7863047.

Sorrentino, Elisa, Anna Federica Spagnuolo, Alessio Portaro, Maria Taverniti, and Elena Cardillo. "Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive

Landscape." In *Proceedings - 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design, IOLTS 2025*. Institute of Electrical and Electronics Engineers Inc., 2025. https://doi.org/10.1109/IOLTS65288.2025.11116851.

Syifaurachman, and Antoni Wibowo. "RISK ASSESSMENT RELATED TO PRIVACY INFORMATION ON ELECTRONIC MONEY SERVER-BASED USING ISO 27001 ISO 27005, ISO 27701." *Journal of Theoretical and Applied Information Technology* 101, no. 3 (2023): 1067 – 1077. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85153800017&partnerID=40&md5=98ca981f35cdafb7790e4b1d8f8ef5fe.

Toapanta, Segundo Moisés T, Marjorie Isanoa Sinche, and Luis Enrique Mafla Gallegos. "A Cyber Environment Approach to Mitigate Vulnerabilities and Threats in an Electoral Process in Ecuador." In *ACM International Conference Proceeding Series*, 97 – 104. Association for Computing Machinery, 2019. https://doi.org/10.1145/3375900.3375914.

Buku

Hadjon, P. M., dkk. (2005). *Pengantar Hukum Administrasi Indonesia*. Yogyakarta: Gadjah Mada University Press.

Ibrahim, J. (2008). *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayu Media Publishing.

Makarim, E. (2017). *Konstitusi dan Telematika: Hak dan Kewajiban Konstitusional Terkait Teknologi Informasi dan Komunikasi*. Jakarta: Badan Penerbit Fakultas Hukum Universitas Indonesia.

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

OECD. (2012). *Keeping it Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes*. OECD Publishing. https://doi.org/10.1787/4df278f7-en

OECD. (2017). *Standard for Automatic Exchange of Financial Account Information in Tax Matters* (2nd ed.). OECD Publishing. https://doi.org/10.1787/9789264267992-en

OECD. (2018). *Standard for Automatic Exchange of Financial Information in Tax Matters: Implementation Handbook* (2nd ed.). OECD Publishing. https://doi.org/10.1787/841e9512-en

OECD. (2023). *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard*. OECD Publishing. https://doi.org/10.1787/896d79d1-en

OECD. (2025). *Consolidated Text of the Common Reporting Standard (2025): Standard for Automatic Exchange of Financial Account Information in Tax Matters*. OECD Publishing. https://doi.org/10.1787/055664b1-en

OECD. (2025). *Peer Review of the Automatic Exchange of Financial Account Information 2025 Update*. OECD/Global Forum on Transparency and Exchange of Information for Tax Purposes.

OECD. (2026). *Terms of Reference for the Confidentiality and Data Safeguards Assessment*. OECD/Global Forum on Transparency and Exchange of Information for Tax Purposes.

Soekanto, S. (1986). *Pengantar Penelitian Hukum*. Jakarta: Penerbit Universitas Indonesia.

Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada.

Sumber Hukum

Indonesia. *Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan beserta perubahan-perubahannya.*

Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya.*

Indonesia. *Undang-Undang Nomor 9 Tahun 2017 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan menjadi Undang-Undang.*

Indonesia. *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.*

Indonesia. *Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan.*

Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.*

Indonesia. *Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.*

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

Kementerian Keuangan Republik Indonesia. *Peraturan Menteri Keuangan Nomor 108 Tahun 2025 tentang Petunjuk Teknis mengenai Akses Informasi Keuangan untuk Kepentingan Perpajakan*.