p-ISSN: 2963-7856| e-ISSN: 2961-9890
Available online at jerkin.org/index.php/jerkin
Jurnal Pengabdian Masyarakat dan Riset Pendidikan
Volume 5 No. 1 Juli-September 2026, 643-648

Tantangan dan Keamanan Data dalam Implementasi Pembaruan Sistem Inti Administrasi Perpajakan (PSIAP)

Nurul Fatwa Ali

Program Studi Magister Kenotariatan, Fakultas Hukum, Universitas 17 Agustus 1945 Semarang, Jl. Pawiyatan Luhur, Bendan Duwur, Kecamatan Gajahmungkur, Kota Semarang, Jawa Tengah
E-mail: nurulftwaa@gmail.com
* Corresponding Author

https://doi.org/10.31004/jerkin.v5i1.7331

ARTICLE INFO

Article history
Received: 05 June 2026
Revised:22 June 2026
Accepted: 08 July 2026

Kata Kunci:
Coretax, keamanan data, perlindungan data pribadi, Direktorat Jenderal Pajak (DJP).

Keywords:
Coretax, data security, personal data protection, Directorate General of Taxes (DJP).

ABSTRACT

Pembaruan Sistem Inti Administrasi Perpajakan (Coretax Administration System) merupakan transformasi digital Direktorat Jenderal Pajak (DJP) yang mengintegrasikan 21 proses bisnis perpajakan melalui satu sumber data (single source of truth), termasuk penggunaan Nomor Induk Kependudukan (NIK) sebagai Nomor Pokok Wajib Pajak (NPWP). Integrasi data berskala besar ini menimbulkan risiko keamanan siber sehingga memerlukan kajian hukum. Penelitian ini bertujuan mengidentifikasi kemampuan regulasi perpajakan dalam melindungi data pribadi wajib pajak, menganalisis risiko serangan siber pada Coretax beserta mitigasinya, serta mengkaji sinkronisasi antara Undang-Undang Perlindungan Data Pribadi (UU PDP) dan kewenangan DJP mengakses data keuangan serta data pihak ketiga. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa UU KUP yang telah diubah oleh UU HPP memberikan dasar hukum kerahasiaan data, namun standar teknis keamanannya masih bergantung pada PMK Nomor 81 Tahun 2024 dan UU PDP. Coretax menghadapi risiko ransomware, kerentanan API, dan ancaman internal yang dimitigasi melalui enkripsi, kontrol akses berbasis peran, dan audit trail. Kewenangan DJP mengakses data pihak ketiga tidak bertentangan dengan UU PDP selama dilakukan secara sah, proporsional, dan akuntabel sebagai pengendali data.

The Coretax Administration System update represents a digital transformation of the Directorate General of Taxes (DGT) that integrates 21 tax business processes through a single source of truth, including the use of the Population Identification Number (NIK) as the Taxpayer Identification Number (NPWP). This large-scale data integration poses cybersecurity risks and requires legal review. This study aims to identify the ability of tax regulations to protect taxpayers' personal data, analyze the risk of cyberattacks on Coretax and their mitigation, and examine the synchronization between the Personal Data Protection Law (PDP Law) and the DGT's authority to access financial and third-party data. The study uses a normative juridical method with a statutory and conceptual approach analyzed descriptively and qualitatively. The results show that the KUP Law, as amended by the HPP Law, provides a legal basis for data confidentiality, but its technical security standards still rely on PMK Number 81 of 2024 and the PDP Law. Coretax faces risks from ransomware, API vulnerabilities, and internal threats, which are mitigated through encryption, role-based access control, and audit trails. The DGT's authority to access third-party data does not conflict with the Data Protection and Data Protection Law, as long as it is exercised legally, proportionally, and accountably as the data controller.

How to Cite: Nurul Fatwa Ali (2026). Tantangan dan Keamanan Data dalam Implementasi Pembaruan Sistem Inti Administrasi Perpajakan (PSIAP), 5(1) 643-648. https://doi.org/10.31004/jerkin.v5i1.7331

PENDAHULUAN

Revolusi Industri 4.0 telah mengubah wajah administrasi publik di seluruh dunia, menjadikannya lebih modern dan serba digital. Digitalisasi bukan lagi sekadar tren, melainkan kebutuhan mendesak untuk menciptakan sistem yang transparan, akuntabel, dan memudahkan masyarakat. Di kancah internasional, Organisation for Economic Co-operation and Development (OECD) telah mendorong konsep Tax Administration 3.0 yang memvisikan sistem perpajakan yang menyatu dengan kehidupan digital masyarakat secara otomatis dan tanpa hambatan (seamless), sehingga urusan pajak dapat diselesaikan secara real-time (Akbar, 2025).

Indonesia menjawab tantangan tersebut melalui peluncuran Pembaruan Sistem Inti Administrasi Perpajakan (PSIAP) yang populer disebut Coretax Administration System. Coretax bukan sekadar penggantian aplikasi lama, melainkan upaya merombak 21 proses bisnis utama Direktorat Jenderal Pajak (DJP) agar lebih adaptif dalam mengawasi kepatuhan pajak di tengah perkembangan teknologi. Urgensi pembaruan ini semakin nyata karena sistem lama mulai kewalahan menangani ledakan data perpajakan, sementara data yang masih terkotak-kotak dan proses manual kerap menghambat optimalisasi tax ratio (Scholastica, 2025). Melalui PSIAP, pemerintah membangun satu sumber data yang akurat (single source of truth), salah satunya dengan menjadikan Nomor Induk Kependudukan (NIK) sebagai Nomor Pokok Wajib Pajak (NPWP), sehingga DJP memiliki profil wajib pajak yang utuh (360-degree view) untuk memetakan potensi pajak secara lebih presisi.

Di balik manfaat tersebut, integrasi data berskala besar membawa risiko yang tidak dapat diabaikan. Pengumpulan berbagai data sensitif dalam satu sistem terpusat menjadikan PSIAP sasaran potensial serangan siber, mengingat data perpajakan tidak hanya memuat informasi finansial tetapi juga identitas pribadi wajib pajak yang bersifat rahasia. Tren serangan siber terhadap institusi publik, seperti ransomware dan kebocoran data (data breach), menunjukkan peningkatan dalam beberapa tahun terakhir (Aska et al., 2024). Apabila sistem keamanan PSIAP tidak dirancang secara optimal, dampaknya tidak hanya berupa kerugian finansial, tetapi juga hilangnya kepercayaan publik terhadap otoritas pajak yang merupakan modal sosial yang sulit dipulihkan.

Selain tantangan teknologi dan regulasi, kesiapan infrastruktur serta sumber daya manusia turut menentukan keberhasilan implementasi PSIAP. Transformasi digital menuntut literasi digital yang memadai, baik dari aparatur pajak maupun wajib pajak sebagai pengguna (Aini, 2025), sementara ketimpangan infrastruktur teknologi di berbagai wilayah Indonesia berpotensi menghambat efektivitas sistem. Tanpa perencanaan mitigasi risiko yang matang, Coretax berisiko menjadi sistem yang canggih secara teknis namun rentan dari sisi keamanan data dan kurang inklusif bagi masyarakat.

Berdasarkan uraian tersebut, permasalahan yang dikaji dalam artikel ini meliputi tiga hal, yaitu sejauh mana regulasi perpajakan saat ini mampu menjamin keamanan data pribadi wajib pajak dalam integrasi sistem Coretax, risiko serangan siber apa saja yang mengintai sistem Coretax beserta kekuatan langkah pengamanan yang diambil DJP, serta bagaimana sinkronisasi antara Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan kewenangan DJP dalam mengakses data keuangan dan data pihak ketiga. Sejalan dengan permasalahan tersebut, kajian ini bertujuan untuk mengidentifikasi kemampuan regulasi perpajakan dalam menjamin keamanan data pribadi wajib pajak, menganalisis risiko serangan siber terhadap sistem Coretax beserta upaya pengamanannya, dan membandingkan sinkronisasi UU PDP dengan kewenangan DJP dalam mengakses data keuangan dan data pihak ketiga, sehingga diharapkan dapat memberikan kontribusi akademis bagi pengembangan tata kelola keamanan data dalam administrasi perpajakan digital di Indonesia.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif (yuridis normatif) yang mengkaji hukum sebagai norma tertulis (*law in books*), dengan menelaah asas hukum, sinkronisasi peraturan perundang-undangan, serta konsep keamanan data dalam konteks administrasi perpajakan digital.

Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) terhadap Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan sebagaimana diubah dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

Menteri Keuangan Nomor 81 Tahun 2024, dan pendekatan konseptual (*conceptual approach*) terhadap konsep kerahasiaan data, keamanan siber, dan perlindungan data pribadi.

Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan di bidang perpajakan dan perlindungan data pribadi, bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian terdahulu, serta bahan hukum tersier berupa artikel berita dan publikasi resmi Direktorat Jenderal Pajak yang relevan dengan implementasi Coretax.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), sedangkan analisis dilakukan secara deskriptif kualitatif dengan metode preskriptif, yaitu menguraikan permasalahan, menghubungkannya dengan norma hukum yang berlaku, kemudian menarik kesimpulan mengenai kesesuaian dan kecukupan regulasi yang ada dalam menjamin keamanan data pada sistem Coretax.

HASIL DAN PEMBAHASAN

Regulasi Perpajakan dalam Menjamin Keamanan Data Pribadi Wajib Pajak pada Sistem Coretax

Prinsip kerahasiaan data merupakan bagian integral dari sistem administrasi pajak di Indonesia sehingga perlindungan data pribadi wajib pajak menjadi sangat penting. Sumber hukumnya adalah Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan (UU KUP) sebagaimana diubah dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan (UU HPP). Salah satu ketentuan utama UU KUP adalah larangan bagi pejabat pajak atau pihak yang terlibat dalam administrasi perpajakan untuk mengungkapkan data dan informasi wajib pajak kepada pihak lain selain yang berwenang sesuai peraturan, sebagai landasan hukum formal yang menegaskan bahwa informasi perpajakan wajib pajak harus tetap rahasia.

Kebijakan teknis dan tata kelola internal DJP memperkuat dasar hukum tersebut dalam praktik administrasi digital seperti Coretax. DJP menegaskan bahwa Sistem Administrasi Coretax bertujuan meningkatkan kualitas administrasi perpajakan dengan menggabungkan berbagai proses bisnis, sambil tetap menjaga kerahasiaan dan keamanan data wajib pajak, sehingga DJP tidak dapat secara langsung mengakses data pribadi seperti saldo rekening atau mutasi tanpa mekanisme dan dasar hukum yang jelas (Arum, Lamsah, & Fitrianingsih, 2025).

Kerahasiaan data ini didukung pula oleh norma sanksi dalam UU KUP. Pasal 41 UU KUP mengatur sanksi pidana terhadap pejabat yang dengan sengaja atau karena kelalaian membocorkan data wajib pajak yang bersifat rahasia, yang menunjukkan bahwa negara memberikan perlindungan hukum konkret terhadap data wajib pajak yang disimpan dan dikelola oleh otoritas pajak (Wildan, 2022).

Meskipun demikian, UU KUP baru memberikan prinsip kerahasiaan tanpa menetapkan standar teknis minimum keamanan data secara rinci, seperti enkripsi dan otentikasi mutlak, sehingga belum cukup mengatur seluruh aspek teknis keamanan siber, perlindungan data pribadi, dan tata kelola pertukaran data dalam sistem digital terintegrasi seperti Coretax. Efektivitas jaminan keamanan data dalam Coretax karenanya sangat bergantung pada tiga hal, yaitu kepatuhan DJP terhadap prinsip kerahasiaan yang ditetapkan UU KUP, termasuk pencatatan aktivitas pengguna (audit trail) dan pengendalian akses sesuai tugas pegawai (Rahayu, 2024), integrasi dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menetapkan definisi lebih rinci tentang data pribadi dan standar pemrosesan data elektronik yang aman (Septiya & Supriyo, 2023), serta peraturan teknis pelaksanaan di lapangan, salah satunya Peraturan Menteri Keuangan Nomor 81 Tahun 2024 tentang Ketentuan Perpajakan dalam Rangka Pelaksanaan Sistem Inti Administrasi Perpajakan (Administrator, 2025).

Dengan demikian, aturan teknis yang jelas dan pengawasan yang konsisten tetap diperlukan untuk menjamin perlindungan yang efektif, meskipun prinsip perlindungan data pribadi wajib pajak telah diatur dalam UU KUP dan ditegaskan dalam kebijakan transformasi digital DJP, agar sistem Coretax mampu menjaga keamanan, kerahasiaan, dan integritas data pribadi wajib pajak di era digital yang semakin kompleks.

Risiko Serangan Siber terhadap Sistem Coretax dan Upaya Pengamanan oleh Direktorat Jenderal Pajak

Coretax Administration System (CTAS) merupakan target yang sangat berharga bagi pelaku kejahatan siber karena menghimpun data dalam skala besar (big data) secara terintegrasi. Faktor internal

organisasi maupun faktor eksternal menjadi sumber risiko, dengan beberapa bentuk ancaman siber yang berpotensi mengintai sistem Coretax.

Pertama, serangan ransomware terstruktur melalui Advanced Persistent Threats (APT) yang kerap menyerang sistem pemerintahan, di mana penjahat siber dapat menyusup ke jaringan selama berbulan-bulan tanpa terdeteksi sebelum meluncurkan ransomware dan jika data pajak terkunci, negara tidak dapat memverifikasi setoran pajak sehingga mengganggu aliran kas negara secara langsung (Bachtiar, 2024). Kedua, kerentanan pada jalur interkoneksi (API security), karena Coretax terhubung dengan banyak lembaga lain seperti bank, Bea Cukai, dan Badan Pertanahan Nasional (BPN), sehingga peretas dapat memasuki sistem DJP melalui salah satu instansi mitra apabila sistem keamanannya lemah (Kurniati, 2023). Ketiga, ancaman internal (insider threat) yang sering kali paling sulit diidentifikasi, mencakup individu yang sengaja menyebarluaskan data untuk keuntungan pribadi hingga pegawai yang tidak sengaja mengunduh dokumen melalui tautan phishing (TechThink, 2024).

Untuk mencegah hal tersebut, DJP dapat mengambil sejumlah langkah mitigasi melalui penerapan sistem keamanan berlapis (defense in depth), yang mencakup pengamanan jaringan dan server, enkripsi data, pengendalian akses berbasis peran (role-based access control), dan pencatatan aktivitas pengguna (audit trail) yang memantau setiap akses dan transaksi data (Rahayu, 2024). Secara ringkas, kategori risiko dan strategi mitigasinya dapat dilihat pada Tabel 1.

Tabel 1. Kategori Risiko dan Strategi Mitigasi Keamanan Siber PSIAP

Kategori Risiko	Deskripsi Ancaman	Dampak	Strategi Mitigasi DJP
Akses Ilegal	Peretasan akun wajib pajak atau petugas melalui credential stuffing atau phishing.	Kebocoran data pribadi dan penyalahgunaan identitas untuk klaim restitusi palsu.	Penerapan Multi-Factor Authentication (MFA) dan sertifikat elektronik.
Integritas Data	Manipulasi data perpajakan oleh pihak luar atau oknum internal yang tidak berwenang.	Data utang pajak atau setoran tidak akurat, merusak keandalan laporan keuangan negara.	Audit trail yang mencatat setiap perubahan data secara permanen dan tidak dapat dihapus.
Ketersediaan Sistem	Serangan DDoS atau ransomware yang melumpuhkan layanan pelaporan pajak daring.	Terhentinya pelayanan publik dan keterlambatan penerimaan kas negara.	Backup data rutin terenkripsi dan penyediaan Disaster Recovery Center (DRC) di berbagai lokasi.
Interkoneksi Data	Kebocoran data pada jalur API saat bertukar informasi dengan bank atau instansi lain.	Paparan data rahasia finansial wajib pajak kepada pihak yang tidak berwenang.	Secure API Gateway dengan enkripsi standar AES-256 pada setiap transaksi data.
Ancaman Internal	Pegawai menyalahgunakan akses untuk mengakses data wajib pajak di luar kewenangannya.	Pelanggaran privasi dan penurunan kepercayaan publik terhadap otoritas pajak.	Privileged Access Management (PAM) dengan akses sesuai kebutuhan tugas (need to know basis).

Tabel 1 menunjukkan bahwa mitigasi risiko keamanan Coretax merupakan adopsi standar ISO/IEC 27001 yang memastikan DJP mengelola keamanan data melalui proses sistematis, mulai dari identifikasi risiko, penerapan kontrol, hingga evaluasi berkala. DJP juga mulai memanfaatkan kecerdasan buatan (Artificial Intelligence/AI) dalam sistem Coretax untuk mengamati pola perilaku pengguna, sehingga aktivitas anomali, misalnya pengunduhan data dalam jumlah besar di luar jam kerja, dapat memicu peringatan otomatis kepada tim keamanan (Security Operation Center/SOC) (Wildan, 2025). Selain itu, penetration testing dan simulasi serangan siber menjadi operasi rutin yang memungkinkan tim teknis menemukan kelemahan sistem sebelum dimanfaatkan oleh pelaku kejahatan siber sesungguhnya.

Meskipun demikian, langkah-langkah pengamanan tersebut tidak selalu berhasil menghadapi ancaman siber yang terus berkembang, sehingga sistem keamanan harus diperbarui secara berkelanjutan

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

melalui audit keamanan dan pengujian kerentanan sistem secara teratur. Tanpa sistem evaluasi dan pengawasan yang konsisten, Coretax tetap rentan terhadap gangguan keamanan, sehingga pengamanan data Coretax merupakan proses berkelanjutan yang memerlukan komitmen kelembagaan dan regulasi yang kuat.

Sinkronisasi Undang-Undang Perlindungan Data Pribadi dengan Kewenangan Direktorat Jenderal Pajak dalam Akses Data Keuangan dan Pihak Ketiga

Persoalan ini menarik karena melibatkan dua rezim hukum yang secara sepintas tampak bertentangan. Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan (UU HPP) memberi DJP wewenang luas untuk memperoleh data keuangan dari bank atau pihak ketiga demi kepentingan negara, sementara Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara ketat melindungi privasi warga negara melalui prinsip legalitas, pembatasan tujuan, proporsionalitas, keamanan, dan akuntabilitas dalam setiap pemrosesan data pribadi.

Meskipun demikian, UU PDP pada dasarnya mengecualikan kepentingan penegakan hukum dan kedaulatan negara, termasuk urusan perpajakan, sehingga DJP tetap bertanggung jawab sebagai pengendali data (data controller). Sinkronisasi antara kedua rezim hukum tersebut dilakukan antara lain melalui pembatasan akses, di mana petugas pajak hanya dapat melihat data yang relevan dengan tugasnya berdasarkan prinsip need to know basis, serta transparansi proses, di mana wajib pajak tetap berhak mengetahui bagaimana data mereka dikelola, meskipun hak untuk menghapus data dibatasi oleh kewajiban perpajakan yang bersifat memaksa secara hukum (lex specialis) (Rahayu, 2024).

Sinkronisasi antara UU PDP dan kewenangan DJP dapat dipahami melalui prinsip bahwa negara dapat memproses data pribadi sepanjang dilakukan untuk kepentingan publik dan pelaksanaan kewenangan yang sah. Pemungutan pajak, sebagai fungsi negara yang penting, memberikan legitimasi hukum bagi DJP untuk mengakses dan mengolah data keuangan dan pihak ketiga, termasuk dalam kerangka integrasi sistem Coretax, sehingga kewenangan tersebut tidak bertentangan secara langsung dengan UU PDP selama dilandasi dasar hukum yang jelas.

Namun demikian, UU PDP tetap mewajibkan lembaga pemerintah sebagai pengendali data pribadi untuk menjamin keamanan data, mencegah penyalahgunaan, dan melindungi hak subjek data, sehingga DJP tidak dapat sepenuhnya mengakses data keuangan tanpa membatasi pemrosesan data hanya untuk tujuan perpajakan, memastikan data tidak bocor, serta membangun mekanisme pertanggungjawaban jika terjadi penyalahgunaan data pribadi. Oleh karena itu, kejelasan teknis dan kebijakan internal DJP diperlukan untuk mengharmoniskan kedua rezim hukum tersebut, sehingga sistem Coretax dapat berfungsi sebagai instrumen efisiensi administrasi perpajakan yang tetap menjaga hak asasi dan kepercayaan publik.

SIMPULAN

Berdasarkan pembahasan mengenai regulasi perpajakan, risiko keamanan siber, serta sinkronisasi Undang-Undang Perlindungan Data Pribadi dengan kewenangan Direktorat Jenderal Pajak dalam implementasi Coretax Administration System, dapat disimpulkan bahwa Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan sebagaimana diubah dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan, yang diperkuat oleh Peraturan Menteri Keuangan terbaru, telah memberikan dasar hukum yang kuat bagi kerahasiaan dan perlindungan data pribadi wajib pajak melalui prinsip kerahasiaan data dan ancaman sanksi pidana.

Kompleksitas sistem Coretax yang terintegrasi dan berbasis big data menimbulkan risiko serangan siber yang signifikan, baik dari ancaman eksternal seperti peretasan dan ransomware maupun ancaman internal berupa penyalahgunaan akses. Meskipun DJP telah menerapkan berbagai langkah pengamanan berbasis standar keamanan internasional, keamanan data tetap memerlukan evaluasi dan pembaruan yang berkelanjutan.

Sinkronisasi antara UU PDP dan kewenangan DJP pada dasarnya tidak bersifat bertentangan, melainkan saling melengkapi. Kewenangan DJP dalam mengakses data keuangan dan pihak ketiga memiliki legitimasi hukum sebagai pelaksanaan fungsi negara, sepanjang dilakukan secara sah, proporsional, terbatas pada tujuan perpajakan, dan disertai tanggung jawab sebagai pengendali data pribadi. Sejalan dengan simpulan tersebut, pemerintah dan DJP perlu menyusun peraturan pelaksana yang lebih rinci mengenai standar keamanan siber dan tata kelola perlindungan data pribadi dalam sistem Coretax, disertai pengawasan internal, audit keamanan berkala, dan peningkatan kapasitas sumber daya

manusia di bidang keamanan siber, serta harmonisasi kebijakan yang berkelanjutan antara rezim perpajakan dan perlindungan data pribadi agar Coretax tetap menjunjung prinsip legalitas, proporsionalitas, dan akuntabilitas dalam menjaga kepercayaan publik.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Dr. Budi Ispriyarso, S.H., M.Hum. selaku dosen pengampu Mata Kuliah Hukum Pajak Program Studi Magister Kenotariatan, Fakultas Hukum, Universitas 17 Agustus 1945 Semarang, atas arahan dan bimbingan yang diberikan dalam penyusunan artikel ini dan segala pihak yang sudah membantu penulis dalam penelitian ini. Semoga artikel ini dapat membantu dan memberikan kontribusi bagi semua pihak yang membutuhkan.

REFERENSI

Administrator. (2025). Coretax 2025, ini yang perlu dilakukan wajib pajak. Pemerintah Pekon Kampung Baru. https://mail.kampungbaru.go.id/artikel/2025/3/21/coretax-2025-ini-yang-perlu-dilakukan-wajib-pajak

Aini, N. (2025). Optimalisasi kepatuhan wajib pajak melalui transformasi digital dan insentif fiskal. Jurnal Ilmu Komunikasi, Administrasi Publik dan Kebijakan Negara, 2(4), 158. https://doi.org/10.62383/komunikasi.v2i4.672

Akbar, L. (2025). Kesiapan Indonesia membangun Tax Administration 3.0. Antara News. https://www.antaranews.com/berita/4799233/kesiapan-indonesia-membangun-tax-administration-30

Arum, M., Lamsah, & Fitrianingsih, D. (2025). Dampak implementasi Coretax System dalam praktik akuntansi pajak dan kepatuhan PPN di Indonesia. Jurnal Kecerdasan Buatan dan Bisnis Digital (RIGGS), 4(4), 1016. https://doi.org/10.31004/riggs.v4i4.3400

Aska, M. F., et al. (2024). Strategi efektif untuk implementasi keamanan siber di era digital. Journal of Information and Information Security (JIFORTY), 5(2), 188–189. https://doi.org/10.56799/ekoma.v4i6.9870

Bachtiar, M. (2024). Apa itu Advanced Persistent Threat? Pengertian & cara mencegahnya. CyberHub Indonesia. https://cyberhub.id/pengetahuan-dasar/advanced-persistent-threat

Kurniati, D. (2023). Pakai API, DJP hubungkan Coretax dengan entitas luar Kemenkeu. DDTC News. https://news.ddtc.co.id/berita/nasional/1795036/pakai-api-djp-hubungkan-coretax-dengan-entitas-luar-kemenkeu

Rahayu, S. K. (2024). Keamanan digital dalam audit pajak: Integrasi cyber security dengan CRM, BDA, dan BI untuk revolusi compliance. UNIKOM Press.

Scholastica, C. A. (2025). Coretax masih bermasalah bikin jeblok pajak di awal tahun, hati-hati target meleset. Inilah.com. https://www.inilah.com/coretax-masih-bermasalah-bikin-jeblok-pajak-di-awal-tahun-hati-hati-target-meleset

Septiya, V., & Supriyo, A. (2023). Perlindungan hukum kerahasiaan data pribadi pada wajib pajak daerah. MENDAPO Journal of Administration Law, 4(2), 177. https://doi.org/10.22437/mendapo.v4i2.25206

TechThink, M. (2024). Mengenal ancaman insider threat: Bahaya dari dalam organisasi. TechThink Hub. https://techthinkhub.co.id/mengenal-ancaman-insider-threat-bahaya-dari-dalam-organisasi/

Wildan, M. (2022). Catat! Ditjen Pajak jamin data PPS tidak bocor, kalau bocor dipenjara. DDTC News. https://news.ddtc.co.id/berita/nasional/36543/catat-ditjen-pajak-jamin-data-pps-tidak-bocor-kalau-bocor-dipenjara

Wildan, M. (2025). DJP sudah punya AI untuk tingkatkan akurasi pengawasan wajib pajak. DDTC News. https://news.ddtc.co.id/berita/nasional/1815621/djp-sudah-punya-ai-untuk-tingkatkan-akurasi-pengawasan-wajib-pajak

Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan sebagaimana diubah dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Menteri Keuangan Nomor 81 Tahun 2024 tentang Ketentuan Perpajakan dalam Rangka Pelaksanaan Sistem Inti Administrasi Perpajakan.

ISSN 2963-7856 (print), ISSN 2961-9890 (online)