

Fakultas Hukum Universitas Riau, Jalan Pattimura Nomor 9 Gobah, Kel. Cinta Raja, Kec. Sail, Pekanbaru, Riau,
Kode Pos 28127. Telp: (+62761)-22539, Fax : (+62761)-21695
E-mail: jihfhur@gmail.com / jih.fh@unri.ac.id
Website: <https://jih.ejournal.unri.ac.id/index.php/JIH/index>

Perlindungan Data Pribadi dalam Teknologi AI: Analisis Peran Hukum dan Kepatuhan Regulasi Bisnis Digital

Tri Vebri Yance^a, Agus Setiawan^b, Rahmi^c, Amaliah Khairunissa^d

^aManajemen Informatika, Politeknik Negeri Sriwijaya, Indonesia, Email: trivebriyance@polsri.ac.id

^bManajemen Informatika, Politeknik Negeri Sriwijaya, Indonesia, Email: agus48@polsri.ac.id

^cManajemen Informatika, Politeknik Negeri Sriwijaya, Indonesia, Email: rahmiyz@polsri.ac.id

^dManajemen Informatika, Politeknik Negeri Sriwijaya, Indonesia, Email: amaliah@polsri.ac.id

Article Info

Article History:

Received : 01-07-2025

Revised : 12-08-2025

Accepted : 20-08-2025

Published : 30-08-2025

Keywords:

Personal data protection

Artificial intelligence

Legal compliance

Digital data

Abstract

Personal data protection. This study aims to examine in depth the legal role in regulating the use of AI that processes personal information, as well as to analyze the compliance challenges faced by business actors in meeting data protection standards. Employing a normative juridical approach supported by literature review, this research evaluates data management principles oriented toward transparency, consent, technical security, and the accountability of electronic system providers. The findings indicate that the inadequacy of legal infrastructure, low levels of privacy literacy, and weak oversight mechanisms have created an imbalance between technological innovation and the protection of data subjects' rights, thereby increasing vulnerabilities to data breaches and potential legal consequences for businesses. This study affirms that strengthening internal policies, implementing auditing mechanisms, and adopting data protection technologies constitute essential instruments for ensuring ongoing compliance. Accordingly, adaptive legal responses and ethically oriented data governance are crucial prerequisites for creating a secure, accountable, and sustainable digital ecosystem in the use of AI technologies.

Informasi Artikel

Histori Artikel:

Diterima : 01-07-2025

Direvisi : 12-08-2025

Disetujui : 20-08-2025

Diterbitkan : 30-08-2025

Kata Kunci:

Perlindungan Data Pribadi

Kecerdasan Buatan

Keatuhan Hukum

Data Digital

Abstrak

Perkembangan teknologi kecerdasan buatan dalam ekosistem bisnis digital telah menghasilkan optimalisasi pemrosesan data dan peningkatan kualitas layanan, namun secara bersamaan menimbulkan problematika fundamental terkait perlindungan data pribadi. Penelitian ini bertujuan mengkaji secara mendalam peran hukum dalam mengatur penggunaan AI yang memproses informasi personal, serta menganalisis tantangan kepatuhan yang dihadapi pelaku usaha dalam memenuhi standar perlindungan data. Melalui pendekatan yuridis normatif berbasis telaah literatur, penelitian ini menilai prinsip-prinsip pengelolaan data yang berorientasi pada transparansi, persetujuan, keamanan teknis, dan akuntabilitas penyelenggara sistem elektronik. Hasil kajian menunjukkan bahwa ketidaksiapan infrastruktur hukum, rendahnya literasi privasi, dan lemahnya mekanisme pengawasan menyebabkan ketidakseimbangan antara inovasi teknologi dan perlindungan hak subjek data, sehingga meningkatkan kerentanan terhadap insiden kebocoran data dan potensi konsekuensi hukum bagi pelaku usaha. Studi ini menegaskan bahwa

PENDAHULUAN

Dalam beberapa tahun terakhir, perkembangan teknologi kecerdasan buatan (AI) telah memberikan dampak signifikan bagi bisnis digital. AI tidak hanya meningkatkan efisiensi operasional, tetapi juga memperkaya pengalaman pengguna melalui personalisasi layanan. Penggunaan AI dalam analitik data memungkinkan perusahaan untuk memahami perilaku pelanggan dengan lebih baik dan merespons kebutuhan mereka secara cepat¹. Namun, dengan semakin melonjaknya penggunaan teknologi ini, muncul berbagai tantangan, khususnya dalam konteks perlindungan data pribadi.

Pentingnya perlindungan data pribadi dalam era digital tidak dapat dipandang sebelah mata, terutama mengingat banyaknya kasus penyalahgunaan data yang terjadi. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai payung hukum untuk mengatur pengelolaan dan perlindungan data pribadi². Meski begitu, tantangan dalam implementasi hukum ini masih tetap ada, seperti lemahnya ketentuan penegakan hukum dan kurangnya pendidikan mengenai hak-hak privasi di kalangan masyarakat³.

Dari sisi regulasi, bisnis digital dihadapkan pada dua tantangan besar: konsistensi kepatuhan terhadap peraturan yang ada dan peningkatan kepercayaan konsumen. Terutama di bidang fintech dan layanan pinjaman online, banyak pelaku usaha yang belum mematuhi standar keamanan yang ditetapkan, sehingga meningkatkan risiko kebocoran⁴. Hal ini menunjukkan perlunya kolaborasi yang lebih baik antara pemerintah, penyedia layanan, dan

¹ Hidayat, R. (2025). Transformasi hukum bisnis di ekosistem digital: studi atas perlindungan data pribadi konsumen. *Riggs Journal of Artificial Intelligence and Digital Business*, 3(4), 46-52. <https://doi.org/10.31004/riggs.v3i4.461>

² Alvember, M. and Asri, D. (2025). Analisis keamanan data pribadi konsumen terhadap regulasi pencantuman nomor induk kependudukan untuk registrasi nomor telepon. *Arus Jurnal Sosial Dan Humaniora*, 5(2), 3017-3026. <https://doi.org/10.57250/ajsh.v5i2.1590>

³ Kartika, R., Nasser, M., & Suswantoro, T. (2025). Analisis yuridis terhadap perlindungan privasi pasien dalam era digital: studi kasus aplikasi satu sehat. *Jurnal Ilmu Hukum Humaniora Dan Politik*, 6(1), 1-8. <https://doi.org/10.38035/jihhp.v6i1.5874>

⁴ Febrian, F., Saputra, I., & Napitupulu, D. (2025). Implikasi hukum terhadap perlindungan data pribadi dalam transaksi fintech. *Rechtsnormen Jurnal Komunikasi Dan Informasi Hukum*, 4(1), 21-30. <https://doi.org/10.56211/rechtsnormen.v4i1.1153>

organisasi masyarakat untuk membangun ekosistem digital yang aman dan responsif terhadap pelanggaran data.

Kebutuhan untuk berbagi data dari pihak ketiga sejatinya membawa implikasi hukum yang besar bagi perlindungan data pribadi. Ketidaksesuaian dalam penerapan standar keamanan antara berbagai platform digital dan lembaga yang terlibat juga dapat memperburuk situasi⁵. Dalam hal ini, regulasi yang lebih adaptif dan pemahaman mendalam mengenai tanggung jawab hukum dari setiap pihak terkait sangat penting untuk memastikan bahwa perlindungan data pribadi terjaga dengan baik di tengah kemajuan teknologi⁶.

Teknologi AI menawarkan banyak peluang baru untuk pertumbuhan bisnis digital, tantangan dalam hal perlindungan data pribadi dan kepatuhan hukum harus ditangani dengan serius. Pembaruan regulasi yang cepat dan pemahaman yang menyeluruh tentang dasar-dasar hukum serta etika dalam penggunaan data menjadi kunci untuk memastikan keberlanjutan dalam perniagaan di era digital yang serba terhubung ini⁷.

ANALISIS DAN PEMBAHASAN

Regulasi Hukum Terkait Perlindungan Data Pribadi dalam Teknologi AI

1. GDPR (General Data Protection Regulation)

GDPR yang mulai berlaku pada tahun 2018 merupakan regulasi data utama di Eropa yang mengatur pengumpulan dan pengelolaan data pribadi. Regulasi ini bertujuan untuk memberikan kontrol lebih kepada individu terkait data mereka dan menetapkan ketentuan-ketentuan ketat bagi organisasi yang mengumpulkan, mengolah, dan menyimpan data pribadi. Dalam konteks teknologi AI, GDPR menerapkan prinsip-prinsip seperti transparansi, tujuan yang jelas, dan minimalisasi data⁸.

Setiap perusahaan yang menggunakan sistem berbasis AI untuk memproses data pribadi harus memastikan bahwa mereka memiliki izin eksplisit dari individu untuk data tersebut,

⁵ Hidayat, R. (2025). Transformasi hukum bisnis di ekosistem digital: studi atas perlindungan data pribadi konsumen. *Riggs Journal of Artificial Intelligence and Digital Business*, 3(4), 46-52. <https://doi.org/10.31004/riggs.v3i4.461>

⁶ Gayo, R. and Ilham, M. (2024). Analisis hukum kewajiban penyedia layanan terhadap perlindungan konsumen dalam bisnis platform digital. *Indonesia Journal of Business Law*, 3(2), 61-68. <https://doi.org/10.47709/ijbl.v3i2.5010>

⁷ Rajgopal, P. (2025). The role of data governance in enabling secure ai adoption. *International Journal of Sustainability and Innovation in Engineering*, 3. <https://doi.org/10.56830/ijsie202501>

⁸ Huda, M., Awaludin, A., & Siregar, H. (2024). Legal challenges in regulating artificial intelligence: a comparative study of privacy and data protection laws. *ijsh*, 1(2), 116-125. <https://doi.org/10.59613/g8dc9v94>

menyampaikan informasi tentang bagaimana data tersebut akan digunakan, dan memberikan hak kepada individu untuk mengakses dan menghapus data mereka⁹. Selain itu, GDPR menetapkan standar keamanan yang harus diterapkan, di mana perusahaan diwajibkan untuk melaporkan kebocoran data dalam waktu 72 jam setelah terjadinya insiden.

2. Undang-Undang Perlindungan Data Pribadi di Indonesia (UU PDP)

UU PDP yang disahkan pada tahun 2022 menjadi landasan hukum utama dalam perlindungan data pribadi di Indonesia. Regulasi ini menetapkan tanggung jawab perusahaan dalam menjaga keamanan dan kerahasiaan data pribadi pelanggan, sama seperti¹⁰. Dalam UU PDP, perusahaan diwajibkan untuk memberikan pemberitahuan yang jelas kepada individu mengenai pengumpulan dan penggunaan data pribadi mereka, serta memperoleh izin yang sah sebelum memproses data tersebut¹¹. UU ini juga memberikan hak-hak tertentu kepada individu, seperti hak untuk mengakses, mengoreksi, dan menghapus data pribadi mereka. Keterbatasan dan tantangan dalam implementasi UU PDP masih ada, termasuk rendahnya literasi hukum di kalangan masyarakat dan lembaga pengawas yang belum sepenuhnya siap¹².

3. Peraturan Perlindungan Konsumen

Peraturan perlindungan konsumen di Indonesia juga mencakup ketentuan yang mengatur pengumpulan dan penggunaan data pribadi. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menegaskan bahwa konsumen berhak untuk mendapatkan informasi yang lengkap dan jujur tentang produk atau layanan yang mereka gunakan, termasuk penggunaan data pribadi¹³. Dalam konteks AI, di mana banyak keputusan bisnis diambil berdasarkan analisis data, perlindungan konsumen menjadi sangat relevan, terutama untuk menghindari eksploitasi dan penyalahgunaan data pribadi yang dapat merugikan konsumen.

⁹ Reddy, H. (2024). Role of ai in security compliance. *Interantional Journal of Scientific Research in Engineering and Management*, 08(11), 1-6. <https://doi.org/10.55041/ijssrem3265>

¹⁰ Arief, L. and Purwanto, R. (2025). Tinjauan yuridis undang-undang perlindungan data pribadi tahun 2022 dalam menangani kebocoran data pelanggan e-commerce. *pk*, 2(3), 85-102. <https://doi.org/10.62383/pk.v2i3.1019>

¹¹ Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20-29. <https://doi.org/10.58812/eslhr.v3i01.351>

¹² Maharani, D., Kusumadara, A., Widhiyanti, H., & Dewantara, R. (2025). Revisiting personal data : ownership theories and comparative legal perspectives from europe, indonesia and the united states. *JDPP*, 7(3), 274. <https://doi.org/10.69554/zmlg9061>

¹³ Priowirjanto, E. (2022). Urgensi pengaturan mengenai artificial intelligence pada sektor bisnis daring dalam masa pandemi covid-19 di indonesia. *Jurnal Bina Mulia Hukum*, 6(2), 254-272. <https://doi.org/10.23920/jbmh.v6i2.355>

4. Peraturan Keamanan Siber dan Perlindungan Data

Regulasi yang mengatur perlindungan data dari ancaman siber juga menjadi aspek penting yang harus dipertimbangkan, terutama dalam penggunaan teknologi AI. Berbagai peraturan, seperti UU ITE (Informasi dan Transaksi Elektronik) dan peraturan lain yang berkaitan dengan keamanan siber, menetapkan langkah-langkah teknis dan administratif yang wajib dipatuhi oleh organisasi untuk melindungi data dari serangan siber¹⁴. Organisasi diwajibkan untuk menerapkan praktik keamanan yang ketat, termasuk enkripsi, kontrol akses, dan deteksi intrusi, guna mengurangi risiko kebocoran dan penyalahgunaan data. Dalam menghadapi tantangan yang terkait dengan kemajuan teknologi, peningkatan regulasi dan adaptasi sistem keamanan yang dinamis sangat penting¹⁵.

Peran Hukum dalam Menjaga Keamanan Data Pribadi dalam Sistem AI

1. Tanggung Jawab Perusahaan terhadap Data Pribadi

Hukum menetapkan tanggung jawab signifikan bagi perusahaan dalam mengelola data pribadi yang digunakan oleh teknologi AI. Dalam kerangka GDPR, organisasi diwajibkan untuk mematuhi prinsip-prinsip pengelolaan data yang mencakup akurasi, kejelasan tujuan pengumpulan, dan batasan penyimpanan¹⁶. Perusahaan harus membangun kebijakan privasi yang jelas dan sistematis untuk menginformasikan pengguna mengenai bagaimana data mereka akan digunakan dan dilindungi. Di Indonesia, UU Perlindungan Data Pribadi (UU PDP) menyatakan bahwa perusahaan yang mengolah data pribadi bertanggung jawab penuh dalam menjaga keamanan dan kerahasiaan data tersebut, termasuk menghadapi konsekuensi hukum jika terjadi pelanggaran terhadap kewajiban ini. Tanggung jawab ini mencakup, antara lain, pelaksanaan langkah-langkah teknis dan administratif yang cukup untuk mencegah kebocoran data¹⁷.

¹⁴ Dash, B., Ansari, M., Sharma, P., & Ali, A. (2022). Threats and opportunities with ai-based cyber security intrusion detection: a review. *International Journal of Software Engineering & Applications*, 13(5), 13-21. <https://doi.org/10.5121/ijsea.2022.13502>

¹⁵ Dmitrieva, E., Balmiki, V., Bhardwaj, N., Kumar, K., Sharma, A., & Shruthi, C. (2024). Security and privacy in ai-driven industry 5.0: experimental insights and threat analysis. *Bio Web of Conferences*, 86, 01097. <https://doi.org/10.1051/bioconf/20248601097>

¹⁶ Ferreira, D., Sousa, M., Bacelar-Silva, G., Frade, S., Antunes, L., Beale, T., ... & Cruz-Correia, R. (2019). Openehr and general data protection regulation: evaluation of principles and requirements. *Jmir Medical Informatics*, 7(1), e9845. <https://doi.org/10.2196/medinform.9845>

¹⁷ Maharani, R. and Prakoso, A. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *Jurnal Usm Law Review*, 7(1), 333-347. <https://doi.org/10.26623/julr.v7i1.8705>

2. Kewajiban Transparansi dan Izin Pengguna

Aspek penting dalam perlindungan data pribadi adalah kewajiban transparansi dan izin dari pengguna. Baik GDPR maupun UU PDP menegaskan bahwa perusahaan harus memberikan informasi yang jelas dan mudah dimengerti kepada individu mengenai pengumpulan dan penggunaan data pribadi mereka. Hal ini diwujudkan dalam bentuk kebijakan privasi yang jelas, dan perusahaan diwajibkan untuk memperoleh izin eksplisit dari pengguna sebelum melakukan pengolahan data pribadi. Kebijakan ini bertujuan untuk meningkatkan kesadaran pengguna akan hak mereka dan memastikan bahwa mereka memiliki kontrol atas informasi yang mereka berikan. Selain itu, perusahaan harus mampu membuktikan bahwa mereka telah mengamankan izin tersebut melalui dokumentasi yang memadai¹⁸.

3. Prinsip Keamanan dan Enkripsi Data

Peran hukum dalam mempromosikan keamanan data, termasuk penggunaan teknologi seperti enkripsi, semakin signifikan dalam konteks pengelolaan data pribadi yang diolah oleh AI. Regulasi seperti GDPR secara eksplisit merekomendasikan penerapan langkah-langkah keamanan yang sesuai, termasuk penggunaan enkripsi untuk melindungi data pribadi¹⁹. Penerapan enkripsi berfungsi untuk mengamankan data yang disimpan maupun yang dikirimkan, sehingga mengurangi risiko kebocoran dan akses tidak sah oleh pihak ketiga. Selain itu, UU PDP juga mengharuskan penyelenggara sistem elektronik untuk menerapkan langkah-langkah keamanan yang memadai, termasuk perlunya sertifikasi keandalan privasi²⁰. Penggunaan teknologi enkripsi sebagai bagian dari infrastruktur keamanan data tidak hanya memenuhi kewajiban hukum tetapi juga membantu perusahaan dalam membangun kepercayaan dengan pengguna terkait integritas data yang mereka kelola²¹.

¹⁸ Nuraziza, S. and Sudirman, W. (2024). Keseimbangan antara inovasi teknologi dan kepatuhan regulasi: tantangan dalam mengintegrasikan artificial intelligence (ai) dalam manajemen keuangan. *MONEY*, 2(1), 47-57. <https://doi.org/10.31004/money.v2i1.2143>

¹⁹ Ferreira, D., Sousa, M., Bacelar-Silva, G., Frade, S., Antunes, L., Beale, T., ... & Cruz-Correia, R. (2019). Openehr and general data protection regulation: evaluation of principles and requirements. *Jmir Medical Informatics*, 7(1), e9845. <https://doi.org/10.2196/medinform.9845>

²⁰ Susanto, H. and Wiyanti, D. (2025). Tanggung jawab penyelenggara fintech terhadap konsumen dalam kasus pembobolan aplikasi dana menurut uu ite 2024 dan uupk 1999. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.18623>

²¹ Ajiboye, K. (2023). Ensuring data security and compliance in ai-powered business applications. *Global Journal of Engineering and Technology Advances*, 15(1), 125-142. <https://doi.org/10.30574/gjeta.2023.15.1.0067>

Kepatuhan Terhadap Regulasi dalam Pengelolaan Data Pribadi AI

1. Strategi Kepatuhan terhadap GDPR dan UU PDP

Perusahaan yang beroperasi dengan teknologi AI menghadapi tantangan besar dalam memastikan kepatuhan terhadap regulasi perlindungan data seperti GDPR dan UU PDP. Untuk memenuhi persyaratan hukum ini, perusahaan sering kali mengimplementasikan berbagai strategi, termasuk pelatihan karyawan mengenai kepatuhan data, serta menerapkan kebijakan privasi dan manajemen risiko yang ketat²². Penyuluhan tentang perlindungan data dan kewajiban hukum membantu meningkatkan kesadaran di kalangan karyawan dan manajemen. Namun, implementasi strategi ini sering kali dihadapkan pada kendala seperti kurangnya sumber daya, kerumitan regulasi yang selalu berubah, dan kebutuhan untuk memodernisasi infrastruktur teknologi informasi²³. Tantangan terbesar adalah menjaga fleksibilitas inovasi sambil tetap mematuhi regulasi yang ketat dan mengadaptasi solusi teknis untuk mengurangi risiko pelanggaran data²⁴.

2. Audit dan Pengawasan Kepatuhan

Auditing dan pengawasan merupakan mekanisme penting untuk memastikan kepatuhan perusahaan terhadap regulasi perlindungan data pribadi. Proses audit ini melibatkan pemeriksaan berkala untuk mengidentifikasi, menilai, dan mengurangi risiko terkait pengelolaan data pribadi²⁵. Pihak ketiga, seperti lembaga audit atau konsultan keamanan siber, sering kali dilibatkan untuk memberikan perspektif independen mengenai kepatuhan dan efektivitas sistem yang ada. Audit juga mencakup tugas untuk memverifikasi bahwa semua kebijakan dan prosedur diikuti, menyesuaikan kebijakan baru sesuai dengan perkembangan teknologi dan perubahan regulasi. Melalui temuan audit, perusahaan dapat meningkatkan tindakan pencegahan dan menegaskan kembali komitmennya terhadap privasi data²⁶. Penekanan pada transparansi dan akuntabilitas dalam laporan audit perlu diperkuat sebagai strategi untuk meningkatkan kepercayaan konsumen.

²² Syailendra, M. and Fitzgerald, S. (2023). Sosialisasi perlindungan data pribadi bagi masyarakat kabupaten indramayu. *JSA*, 1(1), 157-165. <https://doi.org/10.24912/jsa.v1i1.23845>

²³ Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di indonesia dan singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>

²⁴ Bintarawati, F. (2024). The influence of the personal data protection law (uu pdp) on law enforcement in the digital era. *ays*, 1(2), 135-143. <https://doi.org/10.61397/ays.v1i2.92>

²⁵ Raji, I., Xu, P., Honigsberg, C., & Ho, D. (2022). Outsider oversight: designing a third party audit ecosystem for ai governance., 557-571. <https://doi.org/10.1145/3514094.3534181>

²⁶ Paulson, D. and Cannon, B. (2025). Auditing and logging systems for privacy assurance in medical ai pipelines.. <https://doi.org/10.20944/preprints202506.1209.v1>

3. Sanksi Hukum untuk Pelanggaran Kepatuhan

Sanksi hukum untuk pelanggaran kepatuhan terhadap regulasi perlindungan data pribadi dapat bervariasi, mulai dari denda finansial yang signifikan hingga kerugian reputasi yang parah bagi perusahaan²⁷. Di bawah GDPR, perusahaan dapat dikenakan denda hingga 4% dari pendapatan global tahun sebelumnya jika ditemukan pelanggaran berat, sementara UU PDP di Indonesia juga memberikan sanksi yang berat bagi pelanggaran hukum perlindungan data²⁸. Selain denda, pelanggaran regulasi dapat mengakibatkan pencatatan negatif dan kehilangan kepercayaan publik, yang dapat berdampak jangka panjang pada bisnis. Oleh karena itu, penyusunan rencana mitigasi risiko dan kepatuhan yang menyeluruh sangat penting untuk menghadapi dan mencegah potensi konsekuensi dari pelanggaran tersebut²⁹.

Studi Kasus: Pelanggaran Keamanan Data dalam Penggunaan AI di Bisnis Digital

1. Kasus Pelanggaran Data dalam Penggunaan AI

Kasus pelanggaran data yang melibatkan teknologi AI telah menjadi semakin umum dan mencolok. Salah satu contoh nyata berasal dari insiden yang terjadi di perusahaan teknologi besar yang menggunakan AI untuk menganalisis dan mengelola data pelanggan. Dalam insiden tersebut, sistem AI mereka berhasil diretas, mengakibatkan kebocoran data pribadi jutaan pengguna, termasuk informasi sensitif seperti nomor telepon, alamat email, dan rincian keuangan³⁰. Akibat dari pelanggaran ini, perusahaan tidak hanya mengalami kerugian finansial secara langsung tetapi juga harus menghadapi tuntutan hukum dari konsumen yang dirugikan. Dampak tersebut menyebabkan penurunan kepercayaan konsumen dan reputasi perusahaan yang dapat mempengaruhi penjualan dan hubungan bisnis di masa depan³¹.

Dalam skenario hipotetis, anggaplah sebuah perusahaan ritel yang menggunakan AI untuk meningkatkan pengalaman berbelanja secara online. Jika sistem mereka tidak mampu

²⁷ Price, W. and Cohen, I. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37-43. <https://doi.org/10.1038/s41591-018-0272-7>

²⁸ Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di Indonesia dan Singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>

²⁹ Price, W. and Cohen, I. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37-43. <https://doi.org/10.1038/s41591-018-0272-7>

³⁰ Neto, N., Madnick, S., Paula, A., & Borges, N. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality*, 13(1), 1-33. <https://doi.org/10.1145/3439873>

³¹ Junaidi, J. and Fadzil, R. (2024). Urgency of legal personal data protection in e-commerce transactions involving artificial intelligence. *Walisono Law Review (Walrev)*, 6(2), 96-108. <https://doi.org/10.21580/walrev.2024.6.2.25548>

melindungi data pelanggan, dan insiden pelanggaran data mengungkapkan informasi pribadi pelanggan ke publik, hal ini bisa menghasilkan kerugian finansial yang besar serta sanksi hukum dari lembaga pengawas³². Dampak jangka panjang dapat mencakup hilangnya pelanggan, penurunan pendapatan, serta dampak negatif terhadap reputasi merek yang dapat memerlukan waktu bertahun-tahun untuk pulih.

2. Dampak Hukum dan Reputasi terhadap Bisnis

Bagi perusahaan yang gagal melindungi data pribadi dalam aplikasi AI, dampak hukum dapat sangat serius. Pelanggaran GDPR, misalnya, dapat berakibat pada denda finansial hingga 20 juta euro atau 4% dari pendapatan tahunan global perusahaan, tergantung mana yang lebih tinggi³³. Selain itu, terdapat risiko gugatan hukum dari pihak ketiga, termasuk konsumen yang dirugikan yang dapat mengklaim kerugian material dan immaterial akibat kebocoran data tersebut³⁴. Penurunan kepercayaan dari konsumen menjadi salah satu dampak paling berbahaya, karena konsumen cenderung meninggalkan perusahaan yang memiliki reputasi buruk terkait perlindungan data. Laporan menunjukkan bahwa banyak pelanggan akan lebih memilih untuk menghentikan berlangganan layanan ketika mereka merasa tidak aman tentang penanganan data pribadi mereka³⁵.

3. Langkah-langkah Perbaikan Pasca-pelanggaran

Setelah terjadinya pelanggaran data, perusahaan perlu mengambil langkah-langkah perbaikan baik secara hukum maupun teknis untuk memitigasi dampak lebih lanjut dan mencegah insiden di masa depan. Pertama, perusahaan harus segera menginformasikan regulator dan konsumen yang terpengaruh sesuai dengan ketentuan hukum yang berlaku, termasuk melaporkan pelanggaran data kepada otoritas perlindungan data, seperti yang diwajibkan oleh GDPR dan UU PDP³⁶. Selain itu, audit keamanan dan penilaian dampak privasi

³² Pane, M. and Permana, M. (2025). Pertanggungjawaban pidana terhadap pengembang artificial intelligence pada kasus pelanggaran privasi dan data pribadi. *Judge Jurnal Hukum*, 6(03), 467-472. <https://doi.org/10.54209/judge.v6i03.1593>

³³ Mokale, M. (2021). Navigating global data privacy regulations: a guide for telecom operators. *International Journal for Multidisciplinary Research*, 3(4). <https://doi.org/10.36948/ijfmr.2021.v03i04.39051>

³⁴ Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di indonesia dan singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>

³⁵ Piras, L., Al-Obeidallah, M., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B., ... & Zorzino, G. (2019). Defend architecture: a privacy by design platform for gdpr compliance., 78-93. https://doi.org/10.1007/978-3-030-27813-7_6

³⁶ Pandit, H., Ryan, P., Krog, G., Crane, M., & Brennan, R. (2023). Towards a semantic specification for gdpr data breach reporting.. <https://doi.org/10.3233/faia230956>

harus dilakukan untuk mengevaluasi bagaimana pelanggaran terjadi dan langkah-langkah yang perlu diterapkan untuk memperbaiki kebijakan perlindungan data yang ada³⁷.

Langkah teknis yang bisa diterapkan termasuk peningkatan keamanan dalam sistem, penggunaan enkripsi untuk melindungi data sensitif, serta penerapan teknologi pemantauan real-time untuk mendeteksi dan merespons ancaman dengan cepat³⁸. Melalui pendekatan sistematis ini, perusahaan tidak hanya melindungi diri dari sanksi hukum dan risiko reputasi, tetapi juga dapat memperkuat kepercayaan konsumen dan menciptakan lingkungan yang lebih aman dalam penggunaan teknologi AI di masa depan³⁹.

Implikasi Hukum untuk Bisnis yang Menggunakan Teknologi AI

1. Perlindungan Data sebagai Nilai Kompetitif

Perusahaan yang mematuhi regulasi perlindungan data, seperti GDPR dan UU PDP, dapat membangun reputasi yang baik di pasar serta memperkuat kepercayaan konsumen. Dengan memastikan bahwa data pribadi dikelola dengan cara yang etis dan aman, perusahaan dapat menonjol di tengah persaingan yang ketat⁴⁰. Penelitian menunjukkan bahwa kepatuhan terhadap perlindungan data tidak hanya mendatangkan keuntungan hukum, tetapi juga menciptakan nilai kompetitif yang signifikan, karena konsumen cenderung lebih loyal kepada perusahaan yang transparan dalam praktik pengelolaan data mereka⁴¹. Konsumen, terutama di era digital ini, semakin sadar akan isu privasi, sehingga perusahaan yang menempatkan perlindungan data sebagai prioritas strategis dapat memanfaatkan ini untuk menarik dan mempertahankan pelanggan⁴².

³⁷ Piras, L., Al-Obeidallah, M., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B., ... & Zorzino, G. (2019). Defend architecture: a privacy by design platform for gdpr compliance., 78-93. https://doi.org/10.1007/978-3-030-27813-7_6

³⁸ Conduah, A., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: global challenges and solutions. *Digital Health*, 11. <https://doi.org/10.1177/20552076251343959>

³⁹ Masudianto, D. and Barthos, M. (2025). Optimization of personal data rights protection in artificial intelligence era under indonesia's cybersecurity law. *Interdisciplinary Journal and Humanity (Injurity)*, 4(7), 452-462. <https://doi.org/10.58631/injurity.v4i7.1451>

⁴⁰ Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). Eu general data protection regulation: changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. <https://doi.org/10.1016/j.clsr.2017.05.015>

⁴¹ Ahmad, A. (2023). Application of artificial intelligence in improving the efficiency of corporate information systems. *jiem*, 5(2), 1-7. <https://doi.org/10.61992/jiem.v5i2.55>

⁴² Chintoh, G., Segun-Falade, O., Odionu, C., & Ekeh, A. (2025). Challenges and conceptualizing ai-powered privacy risk assessments: legal models for u.s. data protection compliance. *International Journal of Frontline Research in Multidisciplinary Studies*, 5(1), 001-009. <https://doi.org/10.56355/ijfrms.2025.5.1.0036>

2. Kebijakan Internal Perusahaan dalam Keamanan Data

Pengembangan kebijakan internal yang sesuai dengan regulasi, terutama dalam hal pengelolaan data pribadi, adalah langkah krusial bagi perusahaan yang menggunakan teknologi AI. Kebijakan ini harus mencakup langkah-langkah keamanan yang jelas untuk melindungi data, pelatihan untuk staf mengenai prosedur perlindungan data yang tepat, serta evaluasi dan audit berkala untuk memastikan kepatuhan yang berkelanjutan⁴³. Selain itu, organisasi harus menciptakan budaya kesadaran data di antara karyawan, di mana semua anggota tim memahami pentingnya menjaga kerahasiaan dan keamanan informasi pelanggan⁴⁴. Implementasi teknologi seperti enkripsi dan akses terbatas juga harus menjadi bagian dari kebijakan keamanan untuk melindungi data dari ancaman siber.

3. Perspektif Masa Depan: Perkembangan Regulasi dan Teknologi

Memandang ke depan, ada harapan untuk perkembangan regulasi perlindungan data pribadi yang lebih ketat sebagai respons terhadap semakin kompleksnya tantangan yang dihadapi dalam penggunaan AI⁴⁵. Dengan meningkatnya kesadaran publik dan perhatian terhadap privasi, regulator di berbagai belahan dunia diharapkan akan meningkatkan persyaratan kepatuhan, sehingga bisnis harus beradaptasi dengan cepat untuk tetap memenuhi standar yang baru⁴⁶. Ini mungkin termasuk implementasi teknologi baru yang mendukung kepatuhan, seperti otomatisasi proses audit dan pemantauan risiko secara real-time⁴⁷. Integrasi AI dalam pengelolaan data tidak hanya akan menciptakan efisiensi operasional tetapi juga memberikan solusi inovatif untuk mematuhi regulasi yang semakin ketat di masa depan⁴⁸.

⁴³ Benjamin, L., Adegbola, A., Amajuoyi, P., Adegbola, M., & Adeusi, K. (2024). Digital transformation in smes: identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2), 134-153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>

⁴⁴ Pasupuleti, M. (2024). Artificial intelligence in business law: navigating regulation, ethics, and governance., 19-35. <https://doi.org/10.62311/nesx/66203>

Paulson, D. and Cannon, B. (2025). Auditing and logging systems for privacy assurance in medical ai pipelines.. <https://doi.org/10.20944/preprints202506.1209.v1>

⁴⁵ HAMADA, M. and Alhyasat, K. (2023). Artificial intelligence technology to predict the financial crisis in business companies. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 24, 71-82. <https://doi.org/10.55549/epstem.1406233>

⁴⁶ Mou, B. and Yang, X. (2023). Analysis of the role of compliance plan in ai criminal risk prevention-take ai criminal risk in network communication as example. *International Journal of Communication Networks and Information Security (Ijcnis)*, 15(3), 154-167. <https://doi.org/10.17762/ijcnis.v15i3.6242>

⁴⁷ Zahra, Y. (2025). Ensuring data privacy in the age of artificial intelligence. *JOSAPEN*, 3(2), 37-40. <https://doi.org/10.70356/josapen.v3i2.66>

⁴⁸ He, S. (2024). The impact of ai development on the future development of financial industry. *Highlights in Business Economics and Management*, 39, 987-992. <https://doi.org/10.54097/bvxt0d97>

Perkembangan teknologi digital, khususnya kecerdasan buatan (Artificial Intelligence/AI), diproyeksikan akan terus mengalami akselerasi dan penetrasi yang lebih luas dalam berbagai sektor bisnis dan layanan publik. AI tidak lagi hanya berfungsi sebagai alat bantu operasional, tetapi telah menjadi sistem pengambilan keputusan strategis yang memengaruhi aspek ekonomi, sosial, dan hukum. Kondisi ini menuntut adanya regulasi yang bersifat adaptif, antisipatif, dan mampu mengimbangi kecepatan inovasi teknologi tanpa menghambat kreativitas dan daya saing pelaku usaha.

Dari perspektif regulasi, masa depan perlindungan data pribadi dan tata kelola AI diperkirakan akan mengarah pada pendekatan risk-based regulation, yaitu pengaturan berbasis tingkat risiko penggunaan teknologi. Pendekatan ini telah tercermin dalam kebijakan global seperti EU Artificial Intelligence Act, yang mengklasifikasikan sistem AI berdasarkan tingkat risiko terhadap hak asasi manusia dan keamanan publik. Model regulasi ini berpotensi menjadi rujukan bagi negara lain, termasuk Indonesia, dalam menyusun kebijakan AI yang lebih spesifik dan terintegrasi dengan regulasi perlindungan data⁴⁹.

Di Indonesia, UU Perlindungan Data Pribadi (UU PDP) diperkirakan akan terus mengalami penguatan melalui peraturan pelaksana dan kebijakan turunan yang lebih teknis. Ke depan, regulasi tidak hanya berfokus pada aspek kepatuhan administratif, tetapi juga pada penguatan mekanisme pengawasan, penegakan hukum, serta peningkatan kapasitas pelaku usaha dan aparat penegak hukum dalam memahami teknologi AI. Integrasi antara regulasi data, perlindungan konsumen, dan kebijakan ekonomi digital menjadi kebutuhan strategis untuk menciptakan ekosistem digital yang berkelanjutan⁵⁰.

Dari sisi teknologi, tren pengembangan privacy-enhancing technologies (PETs) seperti federated learning, differential privacy, dan secure multi-party computation diprediksi akan semakin berkembang sebagai respons atas tuntutan perlindungan data pribadi. Teknologi-teknologi ini memungkinkan pemanfaatan AI tanpa harus mengorbankan privasi subjek data, sehingga sejalan dengan prinsip privacy by design dan by default yang diamanatkan dalam berbagai regulasi perlindungan data⁵¹.

⁴⁹ European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, Brussels, 2021.

⁵⁰ Alvember, R., dan Asri, D., "Implementasi Undang-Undang Perlindungan Data Pribadi dalam Ekosistem Digital Indonesia," *Jurnal Hukum dan Pembangunan* 55, no. 1 (2025): 45–62.

⁵¹ Taina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies," *Computer Law & Security Review* 34, no. 1 (2018): 134–153.

Selain itu, tuntutan terhadap transparansi dan akuntabilitas algoritma juga akan semakin menguat di masa depan. Konsep explainable AI (XAI) diperkirakan menjadi standar baru dalam pengembangan sistem AI, terutama untuk sektor-sektor berisiko tinggi seperti keuangan, kesehatan, dan layanan publik. Regulasi di masa mendatang kemungkinan akan mewajibkan pelaku usaha untuk mampu menjelaskan logika, tujuan, dan dampak dari keputusan berbasis AI kepada regulator maupun masyarakat luas⁵².

Dengan demikian, masa depan hubungan antara regulasi dan teknologi AI menuntut kolaborasi yang erat antara pemerintah, pelaku industri, akademisi, dan masyarakat sipil. Regulasi yang adaptif dan teknologi yang berorientasi pada etika serta perlindungan hak individu akan menjadi fondasi utama dalam membangun kepercayaan publik dan memastikan bahwa pemanfaatan AI dalam bisnis digital berjalan secara adil, aman, dan berkelanjutan di tengah dinamika transformasi digital global.

KESIMPULAN

Hukum memiliki peran yang krusial dalam melindungi data pribadi dalam sistem berbasis AI. Melalui regulasi seperti General Data Protection Regulation (GDPR) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, perusahaan diberi kerangka hukum untuk memastikan bahwa pengelolaan data pribadi dilakukan secara etis dan aman. Kepatuhan terhadap regulasi ini melindungi hak privasi individu dan menciptakan nilai kompetitif bagi perusahaan di pasar yang semakin memperhatikan isu perlindungan data. Dengan memprioritaskan privasi dan keamanan data, perusahaan dapat membangun reputasi yang positif dan meningkatkan kepercayaan konsumen.

DAFTAR PUSTAKA

- Ahmad, A. (2023). Application of artificial intelligence in improving the efficiency of corporate information systems. *jiem*, 5(2), 1-7. <https://doi.org/10.61992/jiem.v5i2.55>
- Ajiboye, K. (2023). Ensuring data security and compliance in ai-powered business applications. *Global Journal of Engineering and Technology Advances*, 15(1), 125-142. <https://doi.org/10.30574/gjeta.2023.15.1.0067>
- Alvember, M. and Asri, D. (2025). Analisis keamanan data pribadi konsumen terhadap regulasi pencantuman nomor induk kependudukan untuk registrasi nomor telepon. *Arus Jurnal Sosial Dan Humaniora*, 5(2), 3017-3026. <https://doi.org/10.57250/ajsh.v5i2.1590>

⁵² Brent Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi, "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society* 3, no. 2 (2016): 1–21.

- Alvember, R., dan Asri, D., "Implementasi Undang-Undang Perlindungan Data Pribadi dalam Ekosistem Digital Indonesia," *Jurnal Hukum dan Pembangunan* 55, no. 1 (2025): 45–62.
- Arief, L. and Purwanto, R. (2025). Tinjauan yuridis undang-undang perlindungan data pribadi tahun 2022 dalam menangani kebocoran data pelanggan e-commerce. *pk*, 2(3), 85-102. <https://doi.org/10.62383/pk.v2i3.1019>
- Benjamin, L., Adegbola, A., Amajuoyi, P., Adegbola, M., & Adeusi, K. (2024). Digital transformation in smes: identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2), 134-153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>
- Bintarawati, F. (2024). The influence of the personal data protection law (uu pdp) on law enforcement in the digital era. *ays*, 1(2), 135-143. <https://doi.org/10.61397/ays.v1i2.92>
- Brent Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi, "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society* 3, no. 2 (2016): 1–21.
- Chintoh, G., Segun-Falade, O., Odionu, C., & Ekeh, A. (2025). Challenges and conceptualizing ai-powered privacy risk assessments: legal models for u.s. data protection compliance. *International Journal of Frontline Research in Multidisciplinary Studies*, 5(1), 001-009. <https://doi.org/10.56355/ijfrms.2025.5.1.0036>
- Conduah, A., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: global challenges and solutions. *Digital Health*, 11. <https://doi.org/10.1177/20552076251343959>
- Dash, B., Ansari, M., Sharma, P., & Ali, A. (2022). Threats and opportunities with ai-based cyber security intrusion detection: a review. *International Journal of Software Engineering & Applications*, 13(5), 13-21. <https://doi.org/10.5121/ijsea.2022.13502>
- Dmitrieva, E., Balmiki, V., Bhardwaj, N., Kumar, K., Sharma, A., & Shruthi, C. (2024). Security and privacy in ai-driven industry 5.0: experimental insights and threat analysis. *Bio Web of Conferences*, 86, 01097. <https://doi.org/10.1051/bioconf/20248601097>
- European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, Brussels, 2021.
- Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di indonesia dan singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>
- Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di indonesia dan singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>
- Fauzi, M. and Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di indonesia dan singapura. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.19214>
- Febrian, F., Saputra, I., & Napitupulu, D. (2025). Implikasi hukum terhadap perlindungan data pribadi dalam transaksi fintech. *Rechtsnormen Jurnal Komunikasi Dan Informasi Hukum*, 4(1), 21-30. <https://doi.org/10.56211/rechtsnormen.v4i1.1153>
- Ferreira, D., Sousa, M., Bacelar-Silva, G., Frade, S., Antunes, L., Beale, T., ... & Cruz-Correia, R. (2019). Openehr and general data protection regulation: evaluation of principles and requirements. *Jmir Medical Informatics*, 7(1), e9845. <https://doi.org/10.2196/medinform.9845>
- Ferreira, D., Sousa, M., Bacelar-Silva, G., Frade, S., Antunes, L., Beale, T., ... & Cruz-Correia, R. (2019). Openehr and general data protection regulation: evaluation of principles and

- requirements. *Jmir Medical Informatics*, 7(1), e9845. <https://doi.org/10.2196/medinform.9845>
- Gayo, R. and Ilham, M. (2024). Analisis hukum kewajiban penyedia layanan terhadap perlindungan konsumen dalam bisnis platform digital. *Indonesia Journal of Business Law*, 3(2), 61-68. <https://doi.org/10.47709/ijbl.v3i2.5010>
- HAMADA, M. and Alhyasat, K. (2023). Artificial intelligence technology to predict the financial crisis in business companies. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 24, 71-82. <https://doi.org/10.55549/epstem.1406233>
- He, S. (2024). The impact of ai development on the future development of financial industry. *Highlights in Business Economics and Management*, 39, 987-992. <https://doi.org/10.54097/bvxt0d97>
- Hidayat, R. (2025). Transformasi hukum bisnis di ekosistem digital: studi atas perlindungan data pribadi konsumen. *Riggs Journal of Artificial Intelligence and Digital Business*, 3(4), 46-52. <https://doi.org/10.31004/riggs.v3i4.461>
- Hidayat, R. (2025). Transformasi hukum bisnis di ekosistem digital: studi atas perlindungan data pribadi konsumen. *Riggs Journal of Artificial Intelligence and Digital Business*, 3(4), 46-52. <https://doi.org/10.31004/riggs.v3i4.461>
- Huda, M., Awaludin, A., & Siregar, H. (2024). Legal challenges in regulating artificial intelligence: a comparative study of privacy and data protection laws. *ijsh*, 1(2), 116-125. <https://doi.org/10.59613/g8dc9v94>
- Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20-29. <https://doi.org/10.58812/eslhr.v3i01.351>
- Junaidi, J. and Fadzil, R. (2024). Urgency of legal personal data protection in e-commerce transactions involving artificial intelligence. *Walisongo Law Review (Walrev)*, 6(2), 96-108. <https://doi.org/10.21580/walrev.2024.6.2.25548>
- Kartika, R., Nasser, M., & Suswantoro, T. (2025). Analisis yuridis terhadap perlindungan privasi pasien dalam era digital: studi kasus aplikasi satu sehat. *Jurnal Ilmu Hukum Humaniora Dan Politik*, 6(1), 1-8. <https://doi.org/10.38035/jihhp.v6i1.5874>
- Maharani, D., Kusumadara, A., Widhiyanti, H., & Dewantara, R. (2025). Revisiting personal data : ownership theories and comparative legal perspectives from europe, indonesia and the united states. *JDPP*, 7(3), 274. <https://doi.org/10.69554/zmlg9061>
- Maharani, R. and Prakoso, A. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *Jurnal Usm Law Review*, 7(1), 333-347. <https://doi.org/10.26623/julr.v7i1.8705>
- Masudianto, D. and Barthos, M. (2025). Optimization of personal data rights protection in artificial intelligence era under indonesia's cybersecurity law. *Interdisciplinary Journal and Hummanity (Injurity)*, 4(7), 452-462. <https://doi.org/10.58631/injurity.v4i7.1451>
- Mokale, M. (2021). Navigating global data privacy regulations: a guide for telecom operators. *International Journal for Multidisciplinary Research*, 3(4). <https://doi.org/10.36948/ijfmr.2021.v03i04.39051>
- Mou, B. and Yang, X. (2023). Analysis of the role of compliance plan in ai criminal risk prevention-take ai criminal risk in network communication as example. *International Journal of Communication Networks and Information Security (Ijcnis)*, 15(3), 154-167. <https://doi.org/10.17762/ijcnis.v15i3.6242>
- Neto, N., Madnick, S., Paula, A., & Borges, N. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality*, 13(1), 1-33. <https://doi.org/10.1145/3439873>

- Nuraziza, S. and Sudirman, W. (2024). Keseimbangan antara inovasi teknologi dan kepatuhan regulasi: tantangan dalam mengintegrasikan artificial intelligence (ai) dalam manajemen keuangan. *MONEY*, 2(1), 47-57. <https://doi.org/10.31004/money.v2i1.2143>
- Pandit, H., Ryan, P., Krog, G., Crane, M., & Brennan, R. (2023). Towards a semantic specification for gdpr data breach reporting.. <https://doi.org/10.3233/faia230956>
- Pane, M. and Permana, M. (2025). Pertanggungjawaban pidana terhadap pengembang artificial intelligence pada kasus pelanggaran privasi dan data pribadi. *Jurnal Hukum*, 6(03), 467-472. <https://doi.org/10.54209/judge.v6i03.1593>
- Pasupuleti, M. (2024). Artificial intelligence in business law: navigating regulation, ethics, and governance., 19-35. <https://doi.org/10.62311/nex/66203>
- Paulson, D. and Cannon, B. (2025). Auditing and logging systems for privacy assurance in medical ai pipelines.. <https://doi.org/10.20944/preprints202506.1209.v1>
- Paulson, D. and Cannon, B. (2025). Auditing and logging systems for privacy assurance in medical ai pipelines.. <https://doi.org/10.20944/preprints202506.1209.v1>
- Piras, L., Al-Obeidallah, M., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B., ... & Zorzino, G. (2019). Defend architecture: a privacy by design platform for gdpr compliance., 78-93. https://doi.org/10.1007/978-3-030-27813-7_6
- Piras, L., Al-Obeidallah, M., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B., ... & Zorzino, G. (2019). Defend architecture: a privacy by design platform for gdpr compliance., 78-93. https://doi.org/10.1007/978-3-030-27813-7_6
- Price, W. and Cohen, I. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37-43. <https://doi.org/10.1038/s41591-018-0272-7>
- Price, W. and Cohen, I. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37-43. <https://doi.org/10.1038/s41591-018-0272-7>
- Priowirjanto, E. (2022). Urgensi pengaturan mengenai artificial intelligence pada sektor bisnis daring dalam masa pandemi covid-19 di indonesia. *Jurnal Bina Mulia Hukum*, 6(2), 254-272. <https://doi.org/10.23920/jbmh.v6i2.355>
- Rajgopal, P. (2025). The role of data governance in enabling secure ai adoption. *International Journal of Sustainability and Innovation in Engineering*, 3. <https://doi.org/10.56830/ijisie202501>
- Raji, I., Xu, P., Honigsberg, C., & Ho, D. (2022). Outsider oversight: designing a third party audit ecosystem for ai governance., 557-571. <https://doi.org/10.1145/3514094.3534181>
- Reddy, H. (2024). Role of ai in security compliance. *Interantional Journal of Scientific Research in Engineering and Management*, 08(11), 1-6. <https://doi.org/10.55041/ijrsrem3265>
- Susanto, H. and Wiyanti, D. (2025). Tanggung jawab penyelenggara fintech terhadap konsumen dalam kasus pembobolan aplikasi dana menurut uu ite 2024 dan uupk 1999. *Bandung Conference Series Law Studies*, 5(2). <https://doi.org/10.29313/bcsls.v5i2.18623>
- Syailendra, M. and Fitzgerald, S. (2023). Sosialisasi perlindungan data pribadi bagi masyarakat kabupaten indramayu. *JSA*, 1(1), 157-165. <https://doi.org/10.24912/jsa.v1i1.23845>
- Taina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies," *Computer Law & Security Review* 34, no. 1 (2018): 134–153.
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). Eu general data protection regulation: changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. <https://doi.org/10.1016/j.clsr.2017.05.015>

Zahra, Y. (2025). Ensuring data privacy in the age of artificial intelligence. JOSAPEN, 3(2), 37-40. <https://doi.org/10.70356/josapen.v3i2.66>