KOMTELKA: Jurnal Komputer Telekomunikasi dan Elektronika, Volume 01 Nomor 1 Tahun 2026
Tersedia *online* di
https://jurnal.rajawalicemerlangabadi.com/index.php/jpek

Perlindungan Hukum terhadap Kebocoran Data Mahasiswa pada Sistem Informasi Akademik Berbasis *Cloud Computing*

Clarissa Reisana Maharani[1], Nurul Hikmah[2], Yuliarman Saragih[3]

[1,2]*Fakultas Hukum,* [3]*Fakultas Teknik*

email: [1]*2510631010102@student.unsika.ac.id,* [2]*2510631010174@student.unsika.ac.id,* [3]*yuliarman@yahoo.com*

Kata kunci:
perguruan
Cloud
Computing
Data
Perlindungan
Akademik

Keywords:
Cloud
Computing
Data
Protection
Academic

ABSTRAK

Adopsi *cloud computing* pada sistem informasi akademik

tinggi turut berpotensi kerentanan keamanan data pribadi mahasiswa, sehingga risiko terjadinya kebocoran informasi kian serius dan memerlukan perhatian khusus. Penelitian ini berguna mengkaji perlindungan hukum terhadap kebocoran data mahasiswa berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sekaligus merumuskan mekanisme perlindungan menyeluruh. Metode penelitian yang digunakan ialah yuridis normatif dengan pendekatan perundang-undangan serta pendekatan konseptual. Berdasarkan hasil penelitian, penerapan *Multi-Factor Authentication*, enkripsi data, *Role-Based Access Control*, dan audit keamanan berkala merupakan langkah krusial yang harus dijalankan perguruan tinggi
selaku pengendali data dalam pertanggungjawaban hukumnya sesuai UU PDP yang telah diterapkan sepenuhnya sejak Oktober 2024.

ABSTRACT

The adoption of cloud computing in higher education academic information systems also poses potential security vulnerabilities for students' personal data, increasing the risk of information leaks and requiring special attention. This research aims to examine legal protection against student data leaks based on Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), while also formulating a comprehensive protection mechanism. The research method used is normative juridical, incorporating both legislative and conceptual approaches. Based on the research results, the implementation of Multi-Factor Authentication, data encryption, Role-Based Access Control, and periodic security audits are crucial steps that must be implemented by higher education institutions as data controllers to meet their legal responsibilities in accordance with the PDP Law, which has been fully implemented since October 2024.

PENDAHULUAN

Laju perkembangan teknologi informasi yang begitu pesat beberapa tahun terakhir telah berdampak besar terhadap tata kelola perguruan tinggi di Indonesia mengelola proses administrasi dan layanan akademiknya. Salah satu wujud nyata dari perubahan ini adalah meluasnya adopsi *cloud computing* sebagai infrastruktur pokok dalam pengoperasian sistem informasi akademik, menggantikan pendekatan konvensional yang berbasis server lokal.[1] Melalui teknologi berbasis awan ini, institusi pendidikan tinggi dapat menekan biaya investasi infrastruktur sekaligus meningkatkan efisiensi pengelolaan data secara terpusat dan saling terhubung.[2]

Tidak semata-mata dari sisi institusi, kehadiran sistem berbasis *cloud* juga memberi
kemudahan signifikan bagi pengguna akhirnya, mahasiswa maupun dosen kini dapat mengakses jadwal kuliah, rekap nilai, hingga berbagai dokumen akademik tanpa batas waktu dan tempat, tanpa terikat ruang dan waktu.[3] Bahkan dalam skala yang lebih luas, teknologi ini terbukti mendukung kolaborasi antar pengguna serta memperkuat aksesibilitas informasi dalam ekosistem akademik secara keseluruhan.

Di balik segala kemudahan yang ditawarkan sistem informasi akademik berbasis *cloud*, tersimpan ancaman yang tidak bisa diabaikan begitu saja, yakni risiko kebocoran data pribadi mahasiswa yang sewaktu-waktu berpotensi terjadi. Kenyataan ini bukan sekadar kekhawatiran teoretis pada Juni 2024, terjadi serangan siber bertipe ransomware yang menyerang Pusat Data Nasional Sementara (PDNS) 2 di Surabaya menyebabkan lumpuhnya puluhan layanan publik[4], termasuk data sekitar 853.393 calon mahasiswa pendaftar KIP-Kuliah yang dilaporkan ikut terdampak.[5] Memasuki awal tahun 2026, situasi kian mengkhawatirkan seiring munculnya dugaan kebocoran puluhan juta data mahasiswa yang beredar dan diperdagangkan secara ilegal di forum gelap (dark web), sehingga memantik keresahan luas di tengah masyarakat termasuk di kalangan komunitas akademik.[6]

Pratama Persadha, ketua lembaga riset siber *Communication & Information System Security Research Center* (CISSReC) menyatakan kebocoran data sejenis ini membuka pintu bagi berbagai kejahatan turunan, seperti penyebaran *spam* iklan, promosi judi online, penawaran pinjaman online hingga modus penipuan melalui telemarketing misalnya pemberitahuan palsu mengenai kemenangan hadiah yang mengharuskan korban mentransfer sejumlah uang terlebih dahulu agar hadiah tersebut dapat dicairkan.[7]

Sistem informasi akademik berbasis *cloud* mengelola beragam jenis data mahasiswa, mulai dari identitas kependudukan seperti NIK, nomor induk mahasiswa, rekam jejak penilaian dan aktivitas perkuliahan, informasi keuangan terkait beasiswa, hingga data biometrik yang berkategori sangat sensitif. Keberagaman dan sensitivitas data tersebut memposisikannya secara tegas dalam golongan data pribadi yang harus memperoleh perlindungan hukum, sebagaimana diatur secara komprehensif dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), sebagai regulasi yang terbentuk dari amanat konstitusional Pasal 28G ayat (1) UUD 1945 guna memastikan hak setiap warga negara atas perlindungan diri dan data pribadinya.[8] Lebih dari sekadar terbit di atas kertas, UU PDP kini telah sepenuhnya berlaku dan mengikat secara hukum sejak 17 Oktober 2024, setelah masa transisi dua tahun yang diberikan kepada seluruh pihak yang berkepentingan untuk menyesuaikan sistem dan tata kelola data mereka.[9] Artinya, perguruan tinggi sebagai institusi yang sehari-hari mengelola data mahasiswa dalam jumlah besar tidak lagi memiliki ruang toleransi. Mereka kini terikat kewajiban hukum untuk menerapkan standar keamanan teknis dan administratif yang ketat, dan apabila lalai, dapat dihadapkan pada sanksi administratif hingga ancaman pidana sebagaimana diatur dalam ketentuan UU PDP.[10]

Ironisnya, di tengah semakin kuatnya arus digitalisasi dan mandat hukum yang sudah berlaku penuh, kondisi riil di lapangan justru memperlihatkan potret yang masih jauh dari harapan ideal, sejumlah perguruan tinggi di Indonesia masih belum mempunyai sistem keamanan data yang benar-benar andal, baik dari sisi infrastruktur teknologi maupun kelembagaan pengelolaannya. Situasi ini diperburuk oleh kenyataan bahwa

tingkat kematangan keamanan informasi di setiap kampus sangat tidak merata, karena sepenuhnya ditentukan pada seberapa serius masing-masing institusi membangun tata kelola internalnya sendiri kampus yang satu bisa saja sudah memiliki kebijakan keamanan yang relatif baik, sementara yang lain masih beroperasi tanpa audit, tanpa monitoring berkala, dan tanpa literasi keamanan siber yang memadai bagi civitas akademikanya. Oleh sebab itu, penguatan kebijakan keamanan data, peningkatan kesadaran serta literasi terkait keamanan siber di lingkungan kampus, serta penerapan standar manajemen keamanan informasi seperti ISO/IEC 27001 bukan lagi sekadar pilihan, melainkan sebuah kebutuhan yang sudah mendesak dan tidak bisa ditunda.[11] Berangkat dari kondisi inilah penelitian ini disusun dengan tujuan untuk melakukan kajiamendalam kerangka perlindungan hukum yang berlaku atas data mahasiswa dalam sistem informasi akademik berbasis *cloud*, memetakan celah-celah keamanan yang masih terbuka, sekaligus merumuskan rekomendasi mekanisme teknis dan regulatif yang lebih komprehensif sebagai kontribusi akademik terhadap penguatan ekosistem perlindungan data pribadi di Indonesia.

Penelitian ini dilatarbelakangi oleh dua persoalan mendasar yang saling berkaitan. Di satu sisi, terdapat pertanyaan mengenai bagaimana wujud perlindungan hukum terhadap kebocoran data pribadi mahasiswa pada sistem informasi akademik berbasis cloud computing apabila ditelaah dari perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Di sisi lain, penelitian ini juga berupaya mengidentifikasi celah-celah keamanan yang masih terbuka dalam sistem informasi akademik berbasis cloud di perguruan tinggi Indonesia, sekaligus merancang mekanisme perlindungan yang bersifat teknis maupun regulatif secara komprehensif guna mencegah terjadinya kebocoran data pribadi mahasiswa.

Bertolak dari dua persoalan tersebut, penelitian ini dibangun di atas tujuan yang saling melengkapi. Pertama, penelitian ini bertujuan mengkaji dan menganalisis secara mendalam bentuk perlindungan hukum yang dapat

diimplementasikan oleh mahasiswa selaku subjek data dalam menghadapi ancaman kebocoran data pribadi yang tersimpan pada sistem informasi akademik berbasis cloud computing, dengan berpijak pada kerangka normatif Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi beserta implikasinya bagi perguruan tinggi sebagai pengendali data. Kedua, penelitian ini bertujuan memetakan secara sistematis celah keamanan dalam tata kelola sistem informasi akademik berbasis cloud di lingkungan perguruan tinggi Indonesia, sekaligus merumuskan rekomendasi mekanisme perlindungan yang berdimensi ganda, yakni dari sisi teknis melalui penerapan standar seperti ISO/IEC 27001, maupun dari sisi regulatif berupa usulan penguatan kebijakan yang lebih komprehensif dan dapat diimplementasikan secara nyata.

METODE PENELITIAN

Alat Bantu Penelitian

Penelitian ini menggunakan beberapa alat bantu sederhana untuk mendukung analisis perlindungan data mahasiswa pada sistem informasi akademik berteknologi *cloud computing*. Alat bantu yang digunakan tidak berfokus pada aspek pemrograman teknis, melainkan sebagai sarana pendukung analisis hukum dan keamanan data. Google *Scholar* digunakan untuk mencari jurnal, artikel ilmiah, dan referensi akademik terkait perlindungan data pribadi, keamanan siber, serta *cloud computing*. Selain itu, peneliti juga menggunakan situs resmi pemerintah seperti Kementerian Komunikasi dan Digital serta JDIH guna memperoleh peraturan perundang-undangan yang mendukung, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Microsoft Word digunakan dalam proses penyusunan dan pengolahan data penelitian, sedangkan Mendeley digunakan untuk membantu pengelolaan sitasi dan daftar pustaka secara sistematis.

Penelitian ini juga memanfaatkan layanan *cloud computing* seperti Google *Cloud* dan *Amazon Web Services* (AWS) sebagai contoh platform yang banyak digunakan dalam sistem informasi akademik modern.

Standar dan Pendekatan Keamanan

Dalam penelitian ini, penulis menggunakan ISO/IEC 27001 sebagai pedoman fundamental sistem manajemen keamanan informasi karena standar tersebut telah banyak digunakan secara luas dalam perlindungan data digital. Selain itu, penelitian juga merujuk pada prinsip-prinsip perlindungan data yang tercantum dalam *General Data Protection Regulation* (GDPR) sebagai tolak ukur perbandingan implementasi UU PDP di Indonesia.

Jenis dan Pendekatan Penelitian

Penelitian ini menerapkan metode penelitian yuridis normatif dengan pendekatan regulasi perundang-undangan dan pendekatan konseptual. Tujuan dari pendekatan ini adalah untuk meneliti perlindungan hukum terhadap kebocoran data yang melibatkan data mahasiswa dalam sistem informasi akademik berbasis *cloud computing*, selaras dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 perihal Perlindungan Data Pribadi (UU PDP). Studi ini menggunakan pendekatan penelitian yuridis normatif untuk mengkaji peraturan hukum, prinsip-prinsip perlindungan data, dan tanggung jawab pendidikan tinggi sebagai pengolah data terkait perlindungan data mahasiswa. Lebih lanjut, penelitian ini membahas konsep keamanan data digital dalam konteks penggunaan teknologi *cloud computing* di pendidikan tinggi.[12]

Sumber Data

Bahan data dalam penelitian ini bersumber dari sumber hukum primer, sekunder, dan tersier. Sumber hukum primer mencakup Undang-Undang Nomor 27 Tahun 2022 perihal Perlindungan Data Pribadi dan Undang-Undang Nomor 11 Tahun 2008 perihal Informasi dan Transaksi Elektronik, beserta perubahannya. Sumber hukum sekunder didapatkan dari jurnal ilmiah, buku, artikel, dan riset mengenai perlindungan data, keamanan siber, dan implementasi *cloud computing*dalam sistem informasi akademik. Sumber hukum tersier didapatkan dari kamus hukum, ensiklopedia, dan referensi informasi relevan lainnya.

Teknik Pengumpulan Data

Informasi dihimpun melalui kajian kepustakaan, khususnya dengan mengumpulkan dan mempelajari berbagai undang-undang dan peraturan, jurnal akademik, artikel, dan sumber literatur lainnya tentang perlindungan dan keamanan data dalam sistem informasi akademik berbasis *cloud*. Data yang didapatkan selanjutnya dianalisis secara deskriptif dan kualitatif guna memaparkan bentuk- bentuk perlindungan hukum data mahasiswa dan langkah-langkah yang diambil untuk mencegah pelanggaran data dalam

sistem informasi akademik berbasis *cloud*.

Desain Perlindungan Data Mahasiswa pada Sistem *Cloud computing*

Desain perlindungan data yang disajikan dalam studi ini bertujuan untuk mengurangi risiko kebocoran yang melibatkan data mahasiswa dalam sistem informasi akademik berbasis *cloud*. Desain ini menggabungkan perlindungan hukum dengan langkah-langkah keamanan digital yang sederhana namun efektif. Strategi pertama diimplementasikan melalui sistem autentikasi berlapis atau *Multi-Factor Authentication* (MFA) untuk akun mahasiswa, dosen, dan administrator sistem. Penggunaan MFA dimaksudkan untuk mencegah akses ilegal melalui pencurian kata sandi atau penyalahgunaan akun. Selain itu, universitas harus membatasi hak akses ke data menggunakan kontrol *Role-Based Access Control* (RBAC), memastikan bahwa setiap pengguna hanya memiliki akses ke data berdasarkan kewenangan mereka. Strategi kedua adalah enkripsi data dalam sistem penyimpanan *cloud*. Enkripsi berfungsi untuk melindungi data mahasiswa, seperti nomor mahasiswa (NIK/NIM), hasil studi, dan informasi keuangan, dari akses ilegal jika terjadi kegagalan sistem. Strategi ketiga meliputi pengawasan keamanan dan audit sistem secara berkala. Universitas harus melakukan penilaian keamanan terhadap sistem informasi akademiknya untuk mengidentifikasi kelemahan keamanan sejak dini. Selain itu, lembaga pendidikan harus memiliki prosedur untuk menangani kebocoran data selaras dengan Undang-Undang Perlindungan Data Pribadi (UU PDP). Desain perlindungan data ini bertujuan untuk memungkinkan universitas meningkatkan keamanan sistem informasi akademik dan menjamin perlindungan hukum atas data pribadi mahasiswa melalui *cloud computing*.

PEMBAHASAN

Hasil Desain Sistem Perlindungan Data

Berdasarkan analisis tersebut, penelitian ini mengembangkan desain untuk perlindungan data mahasiswa dalam sistem informasi akademik berbasis *cloud computing*. Fokusnya adalah pada keamanan data dan

kepatuhan terhadap ketentuan UU Perlindungan Data Pribadi (UU PDP). Desain sistem yang diusulkan terdiri dari tiga komponen utama: autentikasi pengguna, keamanan data, dan pengawasan sistem. Dalam ranah autentikasi, sistem mengimplementasikan *Multi-Factor Authentication* (MFA) guna meningkatkan keamanan akun pengguna dan mencegah penyalahgunaan data mahasiswa oleh pihak ketiga.[13] Terkait keamanan data, semua data siswa yang disimpan dalam sistem *cloud* dienkripsi untuk memastikan bahwa informasi pribadi seperti nomor identitas siswa (NIK/NIM), prestasi akademik, dan data beasiswa tetap terlindungi jika terjadi serangan siber atau kebocoran data. Selain itu, sistem ini menerapkan pembatasan hak akses berdasarkan peran pengguna (*Role-Based Access Control*).[14] Komponen terakhir adalah pengawasan sistem melalui audit keamanan dan pengawasan rutin aktivitas pengguna. Pengawasan ini berfungsi untuk mendeteksi aktivitas mencurigakan dan mencegah penyalahgunaan data oleh pihak internal dan eksternal.[15]

Tabel 1. Komponen Desain Sistem Perlindungan Data Mahasiswa pada Sistem Informasi Akademik Berbass *Cloud computing*

No	Komponen Desain	Mekanisme yang Diterapkan	Fungsi Perlindungan	Dasar Hukum
1	**Autentikasi Pengguna**	*Multi-Factor Authentication* (MFA)	Mencegah akses ilegal akibat pencurian kata sandi atau penyalahgunaan akun oleh pihak tidak berwenang.	UU No. 27 Tahun 2022 Pasal 35
2	**Pengamanan Data**	Enkripsi data pada sistem penyimpanan	Melindungi data pribadi mahasiswa (NIK, NIM, nilai akademik, data beasiswa) agar tidak terbaca saat terjadi kebocoran.	UU No. 27 Tahun 2022 Pasal 35
3	**Pembatasan Akses**	*Role-Based Access Control* (RBAC)	Memastikan setiap pengguna hanya dapat mengakses data sesuai kewenangannya.	UU No. 27 Tahun 2022 Pasal 34
4	**Pengawasan Sistem**	Audit keamanan dan pemantauan aktivitas pengguna secara berkala	Mendeteksi aktivitas mencurigakan sedini mungkin dan mencegah penyalahgunaan data internal maupun eksternal.	UU No. 27 Tahun 2022 Pasal 46

5	**Penanganan Insiden**	Prosedur notifikasi kebocoran data	Memastikan perguruan tinggi melaporkan insiden kebocoran kepada pemilik data paling lambat sesuai ketentuan yang berlaku.	UU No. 27 Tahun 2022 Pasal 46 Ayat (1)

Analisis Perlindungan Hukum

Hasil penelitian menunjukkan bahwa implementasi sistem keamanan digital harus berjalan beriringan dengan perlindungan hukum terhadap data pribadi mahasiswa. Menurut Undang-Undang No. 27 Tahun 2022 tentang perlindungan data pribadi (UU PDP), perguruan tinggi selaku pengendali data, berkewajiban guna menjamin kerahasiaan dan keamanan data mahasiswa yang dikelola dalam sistem informasi akademik.

Jika terjadi kebocoran data, perguruan tinggi harus memberitahu pemilik data dan bertanggung jawab atas setiap kelalaian dalam pengelolaan sistem keamanan. Oleh karena itu, implementasi konsep perlindungan data yang disajikan dalam penelitian ini dapat menjadi langkah pencegahan untuk mengurangi risiko pelanggaran hukum dan kerugian yang terkait bagi mahasiswa.[16]

Evaluasi Desain

Desain perlindungan data yang diusulkan berkontribusi pada peningkatan keamanan sistem informasi akademik berbasis *cloud computing* melalui kombinasi perlindungan teknis dan perlindungan hukum. Penggunaan MFA, enkripsi data, dan audit keamanan secara berkala membantu Perguruan tinggi meminimalkan risiko kebocoran data terkait data pribadi mahasiswa.

Lebih lanjut, implementasi konsep ini mendukung penerapan prinsip-prinsip keamanan informasi dan perlindungan data di pendidikan tinggi Indonesia, yang semakin bergantung pada teknologi digital dan penyimpanan data berbasis *cloud*.

KESIMPULAN

Berdasarkan temuan penelitian, dapat ditarik kesimpulan bahwa

meskipun penggunaan sistem informasi akademik berbasis *cloud* memberikan kemudahan dalam pengelolaan data mahasiswa, hal ini juga menimbulkan risiko kebocoran data jika sistem keamanan yang memadai tidak diterapkan. Perlindungan hukum data mahasiswa di Indonesia diatur oleh Undang-Undang Nomor 27 Tahun 2022 perihal Perlindungan Data Pribadi (UU PDP). Regulasi ini mewajibkan perguruan tinggi, selaku pengendali data, untuk menjamin keamanan dan kerahasiaan data mahasiswa.

Hasil desain penelitian menunjukkan bahwa implementasi *Multi-Factor Authentication* (MFA), enkripsi data, pembatasan hak akses (*Role-Based Access Control*), dan audit keamanan secara berkala dapat membantu mengurangi risiko kebocoran data pada sistem informasi akademik berbasis *cloud*. Lebih lanjut, kombinasi langkah-langkah keamanan teknis serta kepatuhan terhadap hukum dan peraturan merupakan langkah penting untuk menjamin keamanan data mahasiswa di era digital.

DAFTAR PUSTAKA

[1] A. R. Kambau, "Jurnal Rekayasa Sistem Informasi dan Teknologi Volume 1, No 3-Februari 2024 e-ISSN : 3025-888X PROSES TRANSFORMASI DIGITAL PADA PERGURUAN TINGGI DI INDONESIA," *J. Rekayasa Sist. Inf. dan Teknol.*, vol. 1, no. 3, pp. 126–136, 2024.

[2] D. F. Daulay and R. Sayekti, "STRATEGI MENJAMIN SISTEM KEAMANAN DATA PERPUSTAKAAN DIGITAL UNIVERSITAS NEGERI MEDAN BERBASIS CLOUD COMPUTING," *J. Inform. Teknol. dan Sains*, vol. 7, no. 3, pp. 1464–1472, 2025.

[3] Suwitno *et al.*, "Implementasi Sistem Informasi Akademik Berbasis Cloud Computing System di Pondok Pesantren Khairul Ummah 2 Pekanbaru," *J. Pengabdi. UntukMu NegeRI*, vol. 8, no. 3, pp. 400–408, 2024, doi: 10.37859/jpumri.v8i3.7943.

[4] Fikri Irfan Adristi and Erika Ramadhani, "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede," *Sel. Manaj. J. Mhs. Bisnis Manaj.*, vol. 02, no. 06, pp. 196–212, 2024, [Online]. Available: https://journal.uii.ac.id/selma/index

[5] S. Aranditio, "Terdampak Peretasan PDN, Apa yang Harus Dilakukan Mahasiswa Penerima Beasiswa KIP Kuliah?," *Kompas*, 2024. [Online]. Available: https://www.kompas.id/artikel/kemendikbudristek-pastikan- data-pokok-pendidikan-aman-dari-peretasan-pdn

[6] Mitraberdaya, "58 Juta Data Mahasiswa Diperjualbelikan di Dark Web, Apakah Kampus Anda Sudah Terlindungi?," *PT Mitra Berdaya Optima*, Daerah Istimewa Yogyakarta, 2026. [Online]. Available:

https://mitraberdaya.id/id/news-information/kebocoran-data-mahasiswa-dark-web-iso-21001

[7] CISSRec, "CISSReC: Data Umum Bocor, Ini Potensi Bahayanya," Sep. 19, 2022. [Online]. Available: https://www.cissrec.org/news/detail/1085/CISSReC-Data-Umum-Bocor-Ini-Potensi-Bahayanya.html

[8] *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. 2022. [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[9] I. Today, "Soal Dugaan Kebocoran Data Mahasiswa, Pakar Sistem Keamanan Siber IPB University Ingatkan Risiko Serius," 2026. [Online]. Available: https://ssmi.ipb.ac.id/2026/02/06/soal-dugaan-kebocoran-data-mahasiswa- pakar-sistem-keamanan-siber-ipb-university-ingatkan-risiko-serius/

[10] Syaiful, "Implikasi UU Perlindungan Data Pribadi (PDP): Kewajiban Korporasi dan Hak Warga Negara," *Universitas Medan Area*, Medan, Nov. 22, 2025. [Online]. Available: https://hukum.uma.ac.id/implikasi-uu-perlindungan- data-pribadi-pdp-kewajiban-korporasi-dan-hak-warga-negara/

[11] T. News, "Server Kampus Kebobolan, Ribuan Data Mahasiswa Jadi Sasaran - Ini Langkah Strategis Menjaga dan Meningkatkan Keamanan Informasi," Surabaya, Nov. 12, 2025. [Online]. Available: https://pttati.co.id/news/server- kampus-kebobolan-ribuan-data-mahasiswa-jadi-sasaran-ini-langkah-strategis- menjaga-dan-meningkatkan-keamanan-informasi

[12] J. Efendi and P. Rijadi, *Metode Penelitian Hukum*, Kedua. Jakarta: KENCANA, 2022.

[13] A. Fauzi, I. Nur Aprilla, N. Fauziyyah, and N. Fazriyanti Bachtiar, "Implementasi Multi-Faktor Authentication, Single Sign-on dan Role-Based Access Control dalam Keamanan Sistem Informasi (Studi Literature Review)," vol. 2, no. 1, pp. 33–45, 2025, doi: 10.63217/fibonacci.v2i1.256.

[14] Yuricha and I. K. Phan, "Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.

[15] M. Alfian, R. Rahman, I. Teknologi Bacharuddin Jusuf Habibie, and P. Sulawesi Selatan, "Keamanan Jaringan Pada Perguruan Tinggi," *J. Ris. Sist. Inf.*, vol. 1, no. 3, pp. 59–64, 2024.

[16] N. A. Alfitri, R. Rahmawati, and F. Firmansyah, "Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *J. Soc. Soc.*, vol. 4, no. 2, pp. 92–111, 2024, doi: 10.54065/jss.4.2.2024.511.