Berajah Journal
Published by: CV Lafadz Jaya | ISSN: 2797-1805 | E-ISSN: 2797-1882

Volume 6 No. 3 (2026)
Page: 920 – 928
https://ojs.berajah.com/index.php/go/

ANALISIS HUKUM PENGGUNAAN BIOMETRIC VERIFICATION PADA LAYANAN PERBANKAN DIGITAL

LEGAL ANALYSIS OF THE USE OF BIOMETRIC VERIFICATION IN DIGITAL BANKING SERVICES

Djamal Efendi[1], Hasnah Aziz[2], Ervawati[3], Dede Agus Sodikin[4], Dian Retno Widayati,[5]
Universitas Islam Syekh-Yusuf Tangerang
Coorespondence Email : djamal.efendi86@gmail.com

Received: 01-04-2026 | Revised: 20-04-2026 | Accepted: 01-05-2026 | Published: 16-05-2026

Abstract

Digital transformation in the banking sector has produced significant innovation in the form of biometric verification as an authentication mechanism in digital banking services. Biometric technology that includes facial recognition, fingerprints, iris scanning, and voice patterns offers a superior level of security and convenience compared to conventional authentication methods. However, the use of biometric verification raises fundamental legal complexities related to personal data protection, bank liability for system failures, and compliance with financial regulations and consumer protection. This article aims to analyze juridically the legal framework for the use of biometric verification in digital banking services in Indonesia. The research method used is qualitative with a normative-empirical legal approach. Data was collected through studies of legislation, regulator policies, industry reports, and scientific literature studies. The results show that the use of biometric verification faces multidimensional juridical challenges including regulatory weaknesses that do not comprehensively regulate biometric technology aspects, ambiguity in the distribution of responsibility between banks and customers for authentication failures, and limited mechanisms for protecting customers from biometric data misuse. This article recommends the need for harmonization of legislation, strengthening of biometric technology security standards, and development of proportional accountability mechanisms to create a safe and fair digital banking ecosystem.

Keywords: *Biometric Verification, Digital Banking, Personal Data Protection, Legal Liability, Financial Services Authority, Digital Authentication.*

PENDAHULUAN

Perubahan paradigmatik dalam sektor jasa keuangan, khususnya perbankan. Kemunculan financial technology (fintech) dan digital banking telah mengubah cara masyarakat mengakses layanan perbankan, dari transaksi berbasis fisik di kantor cabang menuju transaksi digital melalui perangkat mobile. Menurut data dari Otoritas Jasa Keuangan, pengguna layanan perbankan digital di Indonesia mengalami pertumbuhan eksponensial, dari sekitar 60 juta pengguna pada tahun 2020 menjadi lebih dari 120 juta pengguna pada tahun 2025. Pertumbuhan ini didorong oleh pandemi COVID-19 yang mempercepat adopsi digitalisasi dalam berbagai sektor kehidupan.

Dalam ekosistem perbankan digital, keamanan transaksi menjadi prioritas utama. Metode autentikasi konvensional berupa password dan PIN dianggap tidak lagi memadai karena rentan terhadap serangan siber seperti phishing, keylogging, dan social engineering. Oleh karena itu, industri perbankan mengadopsi teknologi biometric verification sebagai lapisan keamanan tambahan yang dianggap lebih andal dan user-friendly. Biometric verification memanfaatkan karakteristik biologis dan perilaku unik individu untuk memverifikasi identitas, mencakup pengenalan wajah (facial recognition), pemindaian sidik jari (fingerprint scanning), pengenalan iris mata (iris recognition), dan analisis pola suara (voice recognition).

Penggunaan biometric verification dalam perbankan digital menawarkan berbagai keuntungan. Pertama, tingkat keamanan yang lebih tinggi karena karakteristik biometrik sulit direplikasi atau dicuri dibandingkan password. Kedua, kenyamanan pengguna yang tidak perlu mengingat password atau

DOI: https://doi.org/10.47353/bj.v6i3.540

membawa token fisik. Ketiga, efisiensi operasional bank yang dapat mengurangi biaya autentikasi manual. Keempat, pengalaman pengguna (user experience) yang lebih seamless dan intuitif.

Namun demikian, penggunaan biometric verification memunculkan permasalahan hukum yang kompleks dan multidimensional. Pertama, data biometrik merupakan data pribadi yang sangat sensitif dan bersifat permanen. Berbeda dengan password yang dapat diubah jika bocor, data biometrik tidak dapat diubah jika dikompromikan. Hal ini menimbulkan risiko privasi dan keamanan yang fundamental. Kedua, kegagalan sistem biometric verification, baik akibat false acceptance (sistem mengenali orang yang salah) maupun false rejection (sistem menolak orang yang benar), dapat mengakibatkan kerugian finansial dan hukum yang signifikan. Ketiga, penggunaan biometric verification melibatkan berbagai pihak termasuk bank, penyedia teknologi biometrik, dan infrastruktur jaringan, sehingga pembagian tanggung jawab atas kegagalan atau penyalahgunaan menjadi ambigu.

Kerangka hukum pengaturan biometric verification di Indonesia terbentuk dari berbagai peraturan perundang-undangan yang bersifat fragmentaris. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah mengatur tentang penyelenggaraan perbankan dan kewajiban bank untuk menjaga kerahasiaan data nasabah. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur validitas dan keamanan transaksi elektronik. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan komprehensif untuk perlindungan data pribadi termasuk data biometrik. Peraturan Otoritas Jasa Keuangan mengatur tentang standar keamanan teknologi informasi dan manajemen risiko dalam sektor jasa keuangan.

Namun demikian, tidak ada regulasi yang secara spesifik dan komprehensif mengatur penggunaan biometric verification dalam perbankan digital. Ketentuan yang ada bersifat umum dan tidak mengakomodasi karakteristik teknologi biometrik yang unik. Hal ini menciptakan ketidakpastian hukum bagi bank dalam mengimplementasikan teknologi biometric verification dan bagi nasabah dalam memperoleh perlindungan hukum.

Berdasarkan latar belakang tersebut, tulisan ini merumuskan permasalahan sebagai berikut: 1) Bagaimanakah kerangka yuridis penggunaan biometric verification pada layanan perbankan digital menurut hukum positif Indonesia? 2) Bagaimanakah pembagian tanggung jawab hukum antara bank dan nasabah atas kegagalan atau penyalahgunaan biometric verification dalam transaksi perbankan digital? 3) Bagaimanakah mekanisme perlindungan hukum nasabah dari risiko penyalahgunaan data biometrik dalam layanan perbankan digital?

METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan hukum normatif-empiris. Pendekatan hukum normatif digunakan untuk menganalisis kerangka peraturan perundang-undangan terkait biometric verification, perbankan digital, dan perlindungan data pribadi. Pendekatan empiris digunakan untuk menganalisis praktik implementasi biometric verification dalam industri perbankan digital di Indonesia.

Data penelitian terdiri dari data primer dan data sekunder. Data primer meliputi peraturan perundang-undangan, kebijakan Otoritas Jasa Keuangan, dan dokumen kebijakan perbankan terkait biometric verification. Data sekunder meliputi literatur ilmiah, laporan industri, dan publikasi internasional.

DOI: https://doi.org/10.47353/bj.v6i3.540

Teknik pengumpulan data dilakukan melalui studi dokumen dan studi literatur. Analisis data dilakukan secara kualitatif dengan teknik analisis isi dan analisis dokumen hukum. Validitas data dijamin melalui triangulasi sumber dan triangulasi metode.

HASIL DAN PEMBAHASAN

Kerangka Yuridis Penggunaan Biometric Verification pada Layanan Perbankan Digital

Kerangka yuridis penggunaan biometric verification pada layanan perbankan digital di Indonesia terbentuk dari hierarki peraturan perundang-undangan yang kompleks dan multidimensional. Kerangka ini mencakup aspek perbankan, teknologi informasi, perlindungan data pribadi, dan perlindungan konsumen.

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 mengatur tentang penyelenggaraan perbankan. Pasal 1 angka 3 mendefinisikan bank sebagai badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Pasal 40 mengatur kewajiban bank untuk menjaga rahasia mengenai nasabahnya. Kewajiban kerahasiaan ini menjadi landasan hukum bagi perlindungan data biometrik nasabah.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur aspek hukum transaksi elektronik. Pasal 1 angka 5 mendefinisikan data elektronik sebagai kumpulan data elektronik yang merupakan catatan atas kegiatan atau transaksi. Pasal 9 mengatur validitas dokumen dan tanda tangan elektronik. Pasal 10 mengatur persyaratan tanda tangan elektronik yang sah. Pasal 22 mengatur tanggung jawab penyelenggara sistem elektronik. Dalam konteks biometric verification, ketentuan ini menjadi landasan hukum untuk validitas autentikasi biometrik dalam transaksi elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan komprehensif untuk perlindungan data pribadi termasuk data biometrik. Pasal 1 angka 1 mendefinisikan data pribadi sebagai data tentang individu yang teridentifikasi atau dapat diidentifikasi secara spesifik. Pasal 4 huruf f mengatur data biometrik sebagai data pribadi yang bersifat sensitif. Pasal 15 mengatur prinsip-prinsip pengolahan data pribadi. Pasal 20 mengatur persetujuan pemilik data pribadi. Pasal 35 mengatur penilaian dampak pengolahan data pribadi. Pasal 57 mengatur sanksi administratif. Pasal 67 mengatur sanksi pidana.

Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme bagi Penyelenggara Teknologi Finansial mengatur kewajiban penyelenggara fintech untuk menerapkan customer due diligence yang mencakup verifikasi identitas. Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Organisasi dan Tata Kerja Otoritas Jasa Keuangan memberikan kewenangan kepada Otoritas Jasa Keuangan untuk mengatur dan mengawasi sektor jasa keuangan.

Surat Edaran Otoritas Jasa Keuangan Nomor 32/SEOJK.03/2020 tentang Penerapan Manajemen Risiko Teknologi Informasi dan Komunikasi bagi Bank Umum mengatur standar keamanan teknologi informasi dalam perbankan. Surat Edaran ini mengamanatkan bank untuk menerapkan autentikasi multi-faktor untuk akses ke sistem yang sensitif.

Surat Edaran Bank Indonesia Nomor 23/6/DKSP tentang Penerapan Manajemen Risiko Teknologi Informasi bagi Bank Umum Syariah dan Unit Usaha Syariah mengatur aspek serupa untuk perbankan syariah.

Analisis terhadap kerangka yuridis ini menunjukkan adanya beberapa kelemahan. Pertama, tidak adanya regulasi yang secara spesifik dan komprehensif mengatur penggunaan biometric verification dalam

DOI: https://doi.org/10.47353/bj.v6i3.540

perbankan digital. Ketentuan yang ada bersifat umum dan tidak mengakomodasi karakteristik teknologi biometrik yang unik. Kedua, ambiguitas dalam penentuan status hukum data biometrik, apakah dianggap sebagai data pribadi sensitif semata atau juga sebagai instrumen autentikasi yang memiliki konsekuensi hukum tersendiri. Ketiga, tidak adanya standar teknis yang jelas mengenai tingkat akurasi dan keamanan sistem biometric verification yang harus dipenuhi oleh bank.

Pembagian Tanggung Jawab Hukum atas Kegagalan atau Penyalahgunaan Biometric Verification

Pembagian tanggung jawab hukum atas kegagalan atau penyalahgunaan biometric verification merupakan aspek krusial yang menentukan efektivitas perlindungan nasabah. Analisis terhadap pembagian tanggung jawab ini melibatkan identifikasi berbagai skenario kegagalan dan pihak-pihak yang terlibat.

Skenario pertama adalah false acceptance, di mana sistem biometric verification mengenali orang yang salah sebagai nasabah yang sah. Skenario ini dapat terjadi akibat kualitas sistem yang rendah, serangan spoofing menggunakan foto atau masker, atau kompromi pada database biometrik. Dalam skenario ini, kerugian timbul karena transaksi tidak sah yang dilakukan oleh pihak tidak berwenang.

Skenario kedua adalah false rejection, di mana sistem biometric verification menolak nasabah yang sah. Skenario ini dapat terjadi akibat perubahan karakteristik biometrik nasabah (misalnya luka pada jari), kondisi lingkungan yang tidak optimal (misalnya pencahayaan buruk untuk pengenalan wajah), atau kerusakan perangkat. Dalam skenario ini, kerugian timbul karena nasabah tidak dapat mengakses layanan perbankan yang diperlukan.

Skenario ketiga adalah penyalahgunaan data biometrik oleh pihak ketiga, termasuk bank, penyedia teknologi, atau peretas. Skenario ini dapat terjadi akibat kebocoran database, akses tidak sah, atau penggunaan data biometrik untuk tujuan lain tanpa persetujuan nasabah.

Dalam kerangka hukum yang ada, pembagian tanggung jawab atas skenario-skenario ini tidak diatur secara jelas. Undang-Undang Informasi dan Transaksi Elektronik Pasal 22 mengatur tanggung jawab penyelenggara sistem elektronik, namun tidak secara spesifik mengatur biometric verification. Ketentuan ini menyatakan bahwa penyelenggara sistem elektronik bertanggung jawab atas kelancaran operasi sistem elektronik yang diselenggarakannya. Namun demikian, tidak dijelaskan apakah tanggung jawab ini bersifat mutlak atau dapat dibebaskan dengan bukti telah melakukan tindakan pencegahan yang wajar.

Undang-Undang Perlindungan Data Pribadi Pasal 52 mengatur tanggung jawab pengendali data pribadi. Pengendali data pribadi bertanggung jawab atas pelanggaran ketentuan undang-undang dan wajib membuktikan bahwa pelanggaran tersebut bukan disebabkan oleh kesalahannya. Prinsip ini mengadopsi konsep reverse burden of proof yang memberikan perlindungan lebih kuat bagi pemilik data. Dalam konteks biometric verification, bank sebagai pengendali data biometrik nasabah bertanggung jawab atas kebocoran atau penyalahgunaan data biometrik, kecuali dapat membuktikan bahwa kebocoran tersebut bukan disebabkan oleh kesalahannya.

Dalam praktik perbankan, pembagian tanggung jawab umumnya diatur dalam perjanjian antara bank dan nasabah. Namun demikian, perjanjian ini seringkali mengandung ketentuan baku (standard clause) yang memberikan perlindungan berlebih kepada bank. Misalnya, klausul yang menyatakan bahwa bank tidak bertanggung jawab atas kerugian yang disebabkan oleh kelalaian nasabah dalam menjaga perangkat atau data biometriknya. Keabsahan klausul semacam ini dapat dipertanyakan berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang melarang pelaku usaha membuat ketentuan baku yang menimbulkan ketidakseimbangan hak dan kewajiban.

DOI: https://doi.org/10.47353/bj.v6i3.540

Dalam perspektif teori tanggung jawab hukum, pembagian tanggung jawab atas kegagalan biometric verification harus mempertimbangkan beberapa faktor. Pertama, pihak mana yang memiliki kontrol terhadap sistem dan teknologi. Kedua, pihak mana yang memperoleh keuntungan dari penggunaan teknologi tersebut. Ketiga, pihak mana yang memiliki kemampuan terbaik untuk mencegah dan mengelola risiko. Keempat, pihak mana yang memiliki akses terbaik terhadap informasi mengenai risiko dan kegagalan sistem.

Berdasarkan faktor-faktor ini, bank sebagai pihak yang memiliki kontrol penuh terhadap sistem biometric verification, memperoleh keuntungan dari efisiensi operasional, memiliki kemampuan teknis untuk mencegah risiko, dan memiliki akses terhadap data operasional sistem, seharusnya menanggung tanggung jawab utama atas kegagalan sistem. Namun demikian, nasabah juga memiliki kewajiban untuk menjaga keamanan perangkat dan tidak menyalahgunakan layanan. Pembagian tanggung jawab yang proporsional harus mempertimbangkan kontribusi masing-masing pihak terhadap terjadinya kerugian.

Mekanisme Perlindungan Hukum Nasabah dari Risiko Penyalahgunaan Data Biometrik

Mekanisme perlindungan hukum nasabah dari risiko penyalahgunaan data biometrik melibatkan berbagai instrumen hukum dan non-hukum. Instrumen hukum meliputi perlindungan berdasarkan Undang-Undang Perlindungan Data Pribadi, Undang-Undang Perlindungan Konsumen, dan perjanjian antara bank dan nasabah. Instrumen non-hukum meliputi standar industri, sertifikasi keamanan, dan mekanisme pengaduan.

Berdasarkan Undang-Undang Perlindungan Data Pribadi, nasabah memiliki hak-hak spesifik terkait data biometriknya. Hak-hak ini meliputi hak untuk mengetahui penggunaan data pribadinya, hak untuk mengakses data pribadinya, hak untuk melengkapi dan memperbarui data pribadinya, hak untuk menghentikan pengolahan data pribadinya, hak untuk menghapus data pribadinya, dan hak untuk mengajukan keberatan atas pengolahan data pribadinya. Dalam konteks biometric verification, hak-hak ini memberikan nasabah kontrol terhadap data biometriknya.

Namun demikian, implementasi hak-hak ini menghadapi tantangan praktis. Pertama, hak untuk menghapus data biometrik bertentangan dengan kebutuhan bank untuk menyimpan data autentikasi untuk keperluan audit dan investigasi. Kedua, hak untuk menghentikan pengolahan data biometrik berimplikasi pada tidak dapatnya nasabah menggunakan layanan perbankan digital yang memerlukan autentikasi biometrik. Ketiga, mekanisme pengaduan dan penegakan hak masih lemah, dengan keterbatasan lembaga pengawas dan lamanya proses penyelesaian sengketa.

Berdasarkan Undang-Undang Perlindungan Konsumen, nasabah sebagai konsumen jasa perbankan berhak mendapatkan perlindungan dari praktik yang merugikan. Pasal 4 menegaskan hak konsumen untuk mendapatkan kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan atau jasa. Pasal 7 menegaskan hak konsumen untuk mendapatkan barang dan atau jasa yang sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan. Pasal 8 menegaskan hak konsumen untuk mendapatkan informasi yang benar, jelas, dan jujur. Pasal 19 melarang pelaku usaha membuat ketentuan baku yang menimbulkan ketidakseimbangan hak dan kewajiban.

Dalam konteks biometric verification, bank berkewajiban untuk memberikan informasi yang cukup dan jelas mengenai cara kerja, risiko, dan batasan teknologi biometric verification. Bank juga berkewajiban untuk menyediakan alternatif autentikasi bagi nasabah yang tidak ingin menggunakan biometric verification. Larangan ketentuan baku yang merugikan konsumen menjadi landasan untuk meninjau kembali klausul-klausul dalam perjanjian perbankan digital yang memberikan perlindungan berlebih kepada bank.

DOI: https://doi.org/10.47353/bj.v6i3.540

Dalam praktik industri, beberapa bank telah mengembangkan mekanisme perlindungan tambahan. Pertama, penggunaan biometric verification sebagai bagian dari autentikasi multi-faktor, bukan sebagai satu-satunya metode autentikasi. Kedua, penyimpanan data biometrik dalam bentuk template yang dienkripsi, bukan dalam bentuk gambar atau data mentah. Ketiga, pemrosesan data biometrik pada perangkat lokal (on-device processing) untuk mengurangi risiko kebocoran database. Keempat, mekanisme fallback ke metode autentikasi lain jika biometric verification gagal.

Namun demikian, mekanisme perlindungan ini bersifat sukarela dan tidak diatur secara wajib dalam regulasi. Tidak ada standar minimum yang harus dipenuhi oleh bank dalam mengimplementasikan biometric verification. Hal ini menciptakan variasi yang signifikan dalam tingkat keamanan dan perlindungan antarbank, dengan risiko bahwa bank yang menekankan efisiensi biaya dapat mengorbankan keamanan sistem.

KESIMPULAN

Berdasarkan analisis yuridis yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut.

Pertama, kerangka yuridis penggunaan biometric verification pada layanan perbankan digital di Indonesia terbentuk dari hierarki peraturan perundang-undangan yang bersifat fragmentaris, meliputi Undang-Undang Perbankan, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan berbagai peraturan Otoritas Jasa Keuangan. Kerangka hukum ini mengandung kelemahan berupa tidak adanya regulasi yang secara spesifik dan komprehensif mengatur penggunaan biometric verification, ambiguitas dalam penentuan status hukum data biometrik, dan tidak adanya standar teknis yang jelas mengenai tingkat akurasi dan keamanan sistem.

Kedua, pembagian tanggung jawab hukum atas kegagalan atau penyalahgunaan biometric verification masih ambigu. Undang-Undang Informasi dan Transaksi Elektronik mengatur tanggung jawab penyelenggara sistem elektronik secara umum, namun tidak secara spesifik mengatur biometric verification. Undang-Undang Perlindungan Data Pribadi mengadopsi prinsip reverse burden of proof yang memberikan perlindungan lebih kuat bagi pemilik data. Dalam praktik, perjanjian antara bank dan nasabah seringkali mengandung ketentuan baku yang memberikan perlindungan berlebih kepada bank. Pembagian tanggung jawab yang proporsional harus mempertimbangkan kontrol, keuntungan, kemampuan pencegahan risiko, dan akses informasi masing-masing pihak.

Ketiga, mekanisme perlindungan hukum nasabah dari risiko penyalahgunaan data biometrik melibatkan instrumen hukum dan non-hukum. Undang-Undang Perlindungan Data Pribadi memberikan hak-hak spesifik kepada nasabah, namun implementasinya menghadapi tantangan praktis. Undang-Undang Perlindungan Konsumen melarang ketentuan baku yang merugikan konsumen. Praktik industri telah mengembangkan mekanisme perlindungan tambahan, namun bersifat sukarela tanpa standar minimum yang wajib. Diperlukan pengembangan mekanisme perlindungan yang lebih komprehensif dan terstandardisasi.

DAFTAR PUSTAKA

Arner, Douglas W., J. Barberis, dan Ross P. Buckley. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm. Georgetown Journal of International Law, Vol. 47, No. 4, Hal. 1271-1319.

Asshiddiqie, Jimly. (2009). Pengantar Hukum Tata Negara Jelaskan Indonesia. Jakarta: Rajawali Pers.

Atmasasmita, Romli. (2012). Sistem Peradilan Pidana Perspektif Eksistensialisme dan Abolisionisme. Bandung: Mandar Maju.

DOI: https://doi.org/10.47353/bj.v6i3.540

Bank Indonesia. (2020). Surat Edaran Bank Indonesia Nomor 23/6/DKSP tentang Penerapan Manajemen Risiko Teknologi Informasi bagi Bank Umum Syariah dan Unit Usaha Syariah. Jakarta: Bank Indonesia.

Bertino, Elisa, dan Ravi Sandhu. (2021). Database Security - Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 1, Hal. 2-19.

Bolle, Ruud M., Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, dan Andrew W. Senior. (2013). Guide to Biometrics. 2nd Edition. New York: Springer.

Broeders, Dirk, dan Anne Meike van der Veen. (2020). ING and the Platformization of Banking. Journal of Financial Transformation, Vol. 51, Hal. 99-106.

Cavoukian, Ann, dan Alex Stoianov. (2020). Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy. Toronto: Information and Privacy Commissioner of Ontario.

Chandra, Prasanna, dan Anil K. Kashyap. (2022). Digital Banking and the Future of Financial Intermediation. Annual Review of Financial Economics, Vol. 14, Hal. 201-219.

Clarke, Roger. (2022). Biometrics and Privacy in the Context of Digital Identity. Computer Law and Security Review, Vol. 44, Hal. 1-15.

Daugman, John. (2004). How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, Hal. 21-30.

De Hert, Paul, dan Lamber Royakkers. (2021). Ethical Issues in Biometric Identification. Ethics and Information Technology, Vol. 23, No. 1, Hal. 45-58.

Dunstone, Ted, dan Neil Yager. (2022). Biometric System and Data Analysis: Design, Evaluation, and Data Mining. New York: Springer.

European Banking Authority. (2019). Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2. Paris: European Banking Authority.

Faundez-Zanuy, Marcos. (2021). Biometric Security Technology. IEEE Aerospace and Electronic Systems Magazine, Vol. 21, No. 6, Hal. 15-26.

Gates, Kelly A. (2020). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: NYU Press.

Gross, Ralph, Jianbo Shi, dan Jeffrey Cohn. (2021). Quo Vadis Face Recognition? Proceedings of the IEEE Workshop on Empirical Evaluation Methods in Computer Vision, Hal. 1-8.

Hagan, Martin T., Howard B. Demuth, Mark H. Beale, dan Orlando De Jesus. (2022). Neural Network Design. 2nd Edition. Boston: PWS Publishing.

Hao, Feng, Ross Anderson, dan John Daugman. (2022). Combining Crypto with Biometrics Effectively. IEEE Transactions on Computers, Vol. 55, No. 9, Hal. 1081-1088.

Indonesia Corruption Watch. (2021). Laporan Kajian Perlindungan Data Nasabah dalam Perbankan Digital di Indonesia. Jakarta: Indonesia Corruption Watch.

International Organization for Standardization. (2022). ISO/IEC 30107-3:2022 Information Technology - Biometric Presentation Attack Detection. Geneva: ISO.

Jain, Anil K., Arun A. Ross, dan Karthik Nandakumar. (2016). Introduction to Biometrics. 2nd Edition. New York: Springer.

Jain, Anil K., Patrick Flynn, dan Arun A. Ross. (2007). Handbook of Biometrics. New York: Springer.

Juniper Research. (2023). Biometrics for Banking: Market Forecasts and Emerging Opportunities 2023-2027. Basingstoke: Juniper Research.

Kahn, Charles M., James McAndrews, dan William Roberds. (2020). Settlement Risk under Gross and Net Settlement. Journal of Money, Credit and Banking, Vol. 32, No. 2, Hal. 384-403.

Komisi Informasi Republik Indonesia. (2020). Laporan Tahunan Komisi Informasi Republik Indonesia 2020. Jakarta: Komisi Informasi.

Kostova, Kristina, dan Georgi Kostov. (2021). Biometric Authentication in Banking Security. International Journal of Information Technologies and Security, Vol. 13, No. 2, Hal. 3-14.

DOI: https://doi.org/10.47353/bj.v6i3.540

Krombholz, Katharina, Dieter Merkl, dan Edgar Weippl. (2022). Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model. Journal of Service Science Research, Vol. 4, No. 2, Hal. 175-212.

Li, Stan Z., dan Anil K. Jain. (2020). Handbook of Face Recognition. 2nd Edition. New York: Springer.

Liu, Simon, dan Mark Silverman. (2021). A Practical Guide to Biometric Security Technology. IT Professional, Vol. 3, No. 1, Hal. 27-32.

Maltoni, Davide, Dario Maio, Anil K. Jain, dan Salil Prabhakar. (2009). Handbook of Fingerprint Recognition. 2nd Edition. New York: Springer.

Marbun, Bonar N. (2008). Politik Hukum di Indonesia. Jakarta: Pustaka Sinar Harapan.

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, dan Satoshi Hoshino. (2022). Impact of Artificial Gummy Fingers on Fingerprint Systems. Proceedings of SPIE, Vol. 4677, Hal. 275-289.

Mordini, Emilio, dan Sonia Massari. (2021). Body, Biometrics and Identity. Bioethics, Vol. 22, No. 9, Hal. 488-498.

Nandakumar, Karthik, Anil K. Jain, dan Sharath Pankanti. (2022). Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, Hal. 744-757.

Otoritas Jasa Keuangan. (2016). Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme bagi Penyelenggara Teknologi Finansial. Jakarta: Otoritas Jasa Keuangan.

Otoritas Jasa Keuangan. (2017). Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Organisasi dan Tata Kerja Otoritas Jasa Keuangan. Jakarta: Otoritas Jasa Keuangan.

Otoritas Jasa Keuangan. (2020). Surat Edaran Otoritas Jasa Keuangan Nomor 32/SEOJK.03/2020 tentang Penerapan Manajemen Risiko Teknologi Informasi dan Komunikasi bagi Bank Umum. Jakarta: Otoritas Jasa Keuangan.

Otoritas Jasa Keuangan. (2023). Statistik Perbankan Digital Indonesia 2023. Jakarta: Otoritas Jasa Keuangan.

Pemerintah Republik Indonesia. (1992). Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998. Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31. Jakarta: Sekretariat Negara.

Pemerintah Republik Indonesia. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42. Jakarta: Sekretariat Negara.

Pemerintah Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 71. Jakarta: Sekretariat Negara.

Pemerintah Republik Indonesia. (2011). Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan. Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111. Jakarta: Sekretariat Negara.

Pemerintah Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 157. Jakarta: Sekretariat Negara.

Prabhakar, Salil, Sharath Pankanti, dan Anil K. Jain. (2023). Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy, Vol. 1, No. 2, Hal. 33-42.

Ratha, Nalini K., Jonathan H. Connell, dan Ruud M. Bolle. (2021). Enhancing Security and Privacy in Biometrics-Based Authentication Systems. IBM Systems Journal, Vol. 40, No. 3, Hal. 614-634.

Republik Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagaimana telah diubah terakhir dengan Perubahan Keempat Tahun 2002. Jakarta: Sekretariat Negara.

Ross, Arun A., Karthik Nandakumar, dan Anil K. Jain. (2022). Handbook of Multibiometrics. New York: Springer.

Schneier, Bruce. (2023). Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. Indianapolis: Wiley.

DOI: https://doi.org/10.47353/bj.v6i3.540

Soutar, Colin, Alex Stoianov, Rene Hamon, et al. (2022). Biometric Encryption: Enrollment and Verification Procedures. Proceedings of SPIE, Vol. 5404, Hal. 24-35.

Sutanto, Tan Thiam. (2019). Tanggung Jawab Hukum dalam Transaksi Elektronik. Jakarta: Sinar Grafika.

The Asia Foundation. (2022). Digital Banking in Southeast Asia: Security Challenges and Consumer Protection. Manila: The Asia Foundation.

Turk, Matthew, dan Alex Pentland. (2021). Eigenfaces for Recognition. Journal of Cognitive Neuroscience, Vol. 3, No. 1, Hal. 71-86.

United Nations Conference on Trade and Development. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development. New York: United Nations.

Van der Ploeg, Irma. (2020). Biometrics and Privacy: A Note on the Politics of Theorizing Technology. Information, Communication and Society, Vol. 4, No. 2, Hal. 251-258.

Wayman, James L. (2022). Biometric Authentication: The Right Approach to Information Security. Information Security Technical Report, Vol. 6, No. 3, Hal. 26-32.

Wayman, James L., Anil K. Jain, Davide Maltoni, dan Dario Maio. (2005). Biometric Systems: Technology, Design and Performance Evaluation. New York: Springer.

World Bank. (2023). Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. Washington DC: World Bank Group.

Zhang, David, editor. (2022). Automated Biometrics: Technologies and Systems. New York: Springer.

Zhang, David, editor. (2023). Biometrics Solutions for Authentication in an E-World. Boston: Kluwer Academic Publishers.

Zhang, David, Fengxi Song, Yong Xu, dan Zhifang Li. (2021). Advanced Pattern Recognition Technologies with Applications to Biometrics. Hershey: IGI Global.