CESSIE
Jurnal Ilmiah Hukum
Vol 4 No 4 2025
ISSN: 2830-0092 (Print) ISSN: 2830-0106 (Electronic)
Open Access: https://jurnal.arkainstitute.co.id/index.php/cessie/index

# Etika, Hukum, dan Tata Kelola pada Perusahaan Fintech dalam Pelindungan Data Konsumen

**Pardianto**
[1]Universitas Bakrie, Indonesia
*Email: joepardii99@gmail.com*

**Info Artikel :**
Diterima :
8 Oktober 2025
Disetujui :
10 November 2025
Dipublikasikan :
30 November 2025

**ABSTRAK**

Kerangka Etika Hukum Tata Kelola (EHT) digunakan dalam penelitian ini untuk melihat bagaimana data konsumen dilindungi oleh perusahaan fintech. Dalam penelitian ini, yuridis normatif digunakan untuk menilai kewajiban hukum, prinsip etika, dan mekanisme tata kelola yang berkaitan dengan pengolahan data, proses e-KYC, penagihan, dan pengelolaan risiko teknologi. Penelitian ini kemudian mengintegrasikan kewajiban utama dalam UU PDP dan POJK terkait dengan prinsip seperti *fairness*, minimisasi data, transparansi, privasi secara *default*, dan akuntabilitas model algoritmik. Hasil penelitian menunjukkan bahwa penggunaan perlindungan data fintech masih menghadapi tantangan seperti ketidakseimbangan posisi tawar dalam kontrak baku, ketidakjelasan, bias algoritmik, risiko *Deepfake*, dan kurangnya pengawasan dan tata kelola internal vendor. Metode EHT terbukti efektif untuk melindungi konsumen dengan menggunakan DPIA, model manajemen, kontrol e-KYC berlapis, standar etika penagihan, indikator kinerja, dan peta jalan implementasi. Studi ini menemukan bahwa kerangka integratif EHT dapat memperkuat penerapan hukum yang konsisten, meningkatkan akuntabilitas, dan meningkatkan kepercayaan publik dalam industri fintech Indonesia.

**Kata Kunci: fintech, perlindungan data konsumen, UU PDP, e-KYC, etika bisnis, GCG, OJK.**

***ABSTRACT***

*The Legal Governance Ethics Framework (EHT) was used in this study to examine how consumer data is protected by fintech companies. In this study, normative jurisprudence was used to assess legal obligations, ethical principles, and governance mechanisms related to data processing, e-KYC processes, billing, and technology risk management. This study then integrates the main obligations in the PDP Law and POJK related to principles such as fairness, data minimization, transparency, privacy by default, and algorithmic model accountability. The results show that the use of fintech data protection still faces challenges such as an imbalance of bargaining power in standard contracts, ambiguity, algorithmic bias, Deepfake risks, and a lack of supervision and internal governance of vendors. The EHT method has proven effective in protecting consumers by using DPIA, management models, layered e-KYC controls, ethical collection standards, performance Indicators, and implementation roadmaps. This study finds that the EHT integrative framework can strengthen consistent law enforcement, increase accountability, and enhance public trust in Indonesia's fintech industry.*

***Keywords: fintech, consumer data protection, PDP Law, e-KYC, business ethics, GCG, OJK.***



## PENDAHULUAN

Perkembangan *financial technology* (fintech) di Indonesia membuka jalan baru bagi inklusi dan efisiensi layanan keuangan melalui berbagai model mulai dari *peer-to-peer lending*, dompet digital, *payment gateway*, *paylater*, dan *wealthtech*. Pemrosesan data pribadi dalam skala besar, yang mencakup identitas, perilaku, perangkat, lokasi, dan riwayat transaksi, merupakan "bahan bakar" untuk pengembangan produk, manajemen risiko, dan keputusan otomatis berbasis algoritma. Karena itu, perlindungan data konsumen sangat penting untuk keberlanjutan dan kepercayaan ekosistem fintech [1].

Perlindungan data yang memadai tidak selalu menyertai inovasi digital. Kasus kebocoran yang signifikan, seperti Tokopedia, Cermati, KreditPlus, dan BRI Life, menunjukkan kekurangan kontrol

[1] Asosiasi Fintech Pendanaan Bersama Indonesia, "Pedoman Perilaku Pemberian Layanan Pendanaan Bersama Berbasis Teknologi Informasi Secara Bertanggung Jawab," no. November (2023): 1–15, https://afpi.or.id/assets/document/Pedoman_Perilaku_AFPI_2023_Clean.pdf.

internal. Kebocoran jutaan akun menyebabkan reputasi yang buruk, penipuan dan pencurian identitas, dan peredaran data di pasar gelap. Keamanan data sangat penting untuk operasi karena konsekuensi seperti biaya remediasi, kemungkinan gugatan, dan pengawasan regulator yang semakin ketat[2].

Persoalan etika bisnis pun tampak di layanan pembiayaan digital seperti intimidasi, pelecehan, *doxing*, atau penyebaran data pernah menjadi sorotan dan mengindikasikan lemahnya pengawasan internal serta rendahnya standar perilaku di lapangan. Otoritas Jasa Keuangan (OJK) bersama Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) merespons melalui kode etik penagihan serta kewajiban sertifikasi tenaga penagih. Meski demikian, nilai-nilai etika mesti diinternalisasi dalam budaya organisasi, disertai *incentive alignment* dan mekanisme sanksi yang tegas [3]. *Elektronic Know Your Customer* (e-KYC) mempercepat akses kredit dengan memungkinkan pembukaan akun tanpa pertemuan langsung dan mengurangi biaya melalui biometrik, pengenalan wajah, dan deteksi keaktifan. Tapi bias algoritmik, salah verifikasi, keputusan otomatis yang tidak transparan, dan ancaman *Deepfake* dan identitas buatan muncul. Akibatnya, ada kebutuhan untuk mengimbangi perluasan akses dengan pengurangan risiko melalui *privacy by design/default*, pengurangan data, dan uji *fairness*.

Untuk mengurangi risiko yang terkait dengan pemrosesan data di industri fintech, sistem hukum Indonesia terus diperbarui. UU 27/2022 tentang Pelindungan Data Pribadi menetapkan hak subjek data, aturan pemrosesan, tanggung jawab pengendali dan pemroses, pelaporan insiden, dan sanksi. ITE Act, PP 71/2019, dan PP 80/2019 dilengkapi oleh aturan ini. OJK mengeluarkan POJK 40/2024, yang meningkatkan tata kelola, manajemen risiko, dan permodalan untuk pembiayaan berbasis TI. Di area APU-PPT, POJK 8/2023 menetapkan verifikasi *non-face-to-face*, penilaian risiko, dan pengawasan aktif untuk mencegah penyalahgunaan data dan penipuan identitas pada e-KYC. Perlindungan konsumen didukung oleh POJK 6/2022 dan 22/2023, dan inovasi didorong oleh sandbox regulasi ITSK (POJK 3/2024). Pembentukan LAPS-SJK melalui POJK 61/2020 memperkuat penyelesaian sengketa konsumen[4].

Dimensi tata kelola perusahaan *(Good Corporate Governance*/GCG) menjadi penggerak akuntabilitas agar komitmen etika dan kepatuhan hukum tidak berhenti pada dokumen kebijakan. Praktiknya mencakup pembentukan komite risiko/teknologi, peta jalan manajemen keamanan informasi & siber, *privacy impact assessment*, pengawasan model & data untuk *scoring*, serta uji ketahanan insiden (*table-top exercise*). Dewan perlu memastikan keberadaan *Data Protection Officer* atau fungsi setara yang independen, didukung anggaran, kewenangan, dan akses informasi yang memadai [5]. Untuk memastikan akuntabilitas yang terukur, perusahaan perlu menetapkan indikator kinerja perlindungan data waktu pemenuhan hak akses/koreksi/penghapusan, tingkat penyelesaian keluhan, waktu deteksi dan respons insiden, *tingkat false positive/false negative* verifikasi e-KYC, jumlah temuan audit yang

---

[2] Tempo.Co, "Data KTP Hingga Rekam Medis 2 Juta Nasabah BRI Life Diduga Bocor Dan Dijual," *Tempo.Co*, 2021, tempo.co/ekonomi/data-ktp-hingga-rekam-medis-2-juta-nasabah-bri-life-diduga-bocor-dan-dijual-490216#google_vignette; CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual," *CNN Indonesia*, 2020, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

[3] Asosiasi Fintech Pendanaan Bersama Indonesia, "Pedoman Perilaku Pemberian Layanan Pendanaan Bersama Berbasis Teknologi Informasi Secara Bertanggung Jawab."

[4] Peraturan Pemerintah, "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Lembaran Negara RI" (2022); Peraturan Pemerintah, "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. Lembaran Negara RI" (2019); Peraturan Pemerintah, "Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik. Lembaran Negara RI" (2019); Otoritas Jasa Keuangan, "Pojk 40/2024," 2024, 1–23, https://ojk.go.id/id/regulasi/Pages/POJK-40-Tahun-2024-Layanan-Pendanaan-Bersama-Berbasis-Teknologi-Informasi.aspx; Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10 /Pojk.05/2022 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi," no. 184 (2014): 1–27; Dewan Komisioner OJK, "Otoritas Jasa Keuangan Republik Indonesia," 2015; Jenny Andrea, Yaswirman, and Rembrandt, "Akibat Hukum Penundaan Pengikatan Jaminan Dalam Perjanjian Kredit Modal Kerja Pt. Bank Negara Indonesia (Persero) Tbk," *Van Java Law Journal* 1, no. 01 (2024): 50–79, https://doi.org/10.64578/vjlj.v1i01.72; Peraturan Otoritas Jasa Keuangan, "Peraturan Otorisasi Jasa Keuangan Republik Indonesia Nomor 3 Tahun 2024 Tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan," *Peraturan Otoritas Jasa Keuangan*, 2024.

[5] A Mita, F, "Pedoman Umum Governansi Korporat Indonesia (PUGKI) 2021," *Komite Nasional Kebijakan Governansi*, 2021, 37, https://knkg.or.id/wp-content/uploads/2022/06/PUGKI-2021-LORES.pdf.

ditutup tepat waktu, dan kepatuhan vendor terhadap *service level agreement*. *Penerbitan transparency report*, pelaksanaan *privacy by design checklist*, dan publikasi rencana perbaikan pasca insiden akan memperkuat disiplin internal sekaligus meningkatkan kepercayaan pemangku kepentingan.

Pada level ekosistem, harmonisasi regulasi dan koordinasi pengawasan menjadi kunci. OJK, Kominfo, BI, dan aparat penegak hukum perlu menyelaraskan standar serta menetapkan akuntabilitas yang jelas, termasuk bagi pelaku lintas batas. Asosiasi industri dapat memperkuat praktik melalui pedoman teknis, sertifikasi, dan peningkatan kapasitas. Di sisi konsumen, literasi privasi dan edukasi risiko harus ditingkatkan lewat notifikasi yang mudah dipahami, antarmuka ramah, layanan bantuan responsif, dan mekanisme keluhan yang terhubung dengan LAPS-SJK [6]. Ekosistem fintech menghadapi banyak masalah, seperti kebocoran data yang merusak kepercayaan publik, praktik penagihan tidak etis pada beberapa lending P2P, dan kesenjangan regulasi yang terjadi karena kekurangan sumber daya manusia, ketidaktahuan tentang privasi, dan kurangnya pengawasan vendor. Kondisi menjadi lebih buruk karena masalah e-KYC seperti bias algoritmik, *Deepfake*, dan identitas buatan, serta GCG yang belum optimal, seperti dewan, manajemen risiko, audit internal, dan DPO. Situasi ini menegaskan kebutuhan akan kerangka integratif yang memadukan etika, hukum, dan tata kelola agar kepatuhan tidak menjadi sekadar *"checklist compliance."*

Penelitian Satory mengenai "Perjanjian Baku dan Perlindungan Konsumen", menegaskan kontrak baku kerap merugikan konsumen karena tidak seimbangnya posisi tawar [7]. Dalam buku *Meneroka Relasi Hukum, Negara, dan Budaya*, menjelaskan bahwa regulasi saja tidak cukup tanpa perubahan budaya hukum, khususnya dalam perlindungan konsumen [8]. OECD menekankan peran tata kelola dalam membangun kepercayaan, transparansi, dan akuntabilitas untuk pertumbuhan berkelanjutan [9].

Studi pengguna fintech di Indonesia menunjukkan bahwa meskipun banyak orang tertarik dengan fintech, masalah hukum dan keamanan *(privacy, data)* terus menghalangi adopsi [10]. Studi normatif tentang sistem skoring kredit otomatis fintech menunjukkan bahwa, meskipun undang-undang seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sudah ada, mereka seringkali tidak diterapkan dengan baik, terutama dalam hal pemberitahuan, pembatasan tujuan, dan proses keberatan data [11]. Menurut penelitian dan penelitian algoritma di seluruh dunia, ketidakadilan dan bias dalam model pembelajaran mesin adalah masalah yang nyata. Misalnya, bias demografi biometrik dapat mendiskriminasi kelompok tertentu. Oleh karena itu, audit keadilan dan kontrol etis sangat penting [12]. Studi tentang etika dan kepemimpinan fintech menekankan bahwa kemajuan teknologi harus diiringi dengan kepatuhan etika dan tata kelola untuk mempertahankan kepercayaan publik [13]. Banyak penelitian membahas aspek-aspek tersebut secara terpisah, seperti fokus pada persepsi risiko konsumen, etika fintech, atau tata kelola AI. Namun, hanya sedikit penelitian yang

---

[6] OJK, "Peraturan Otoritas Jasa Keuangan Nomor 61/POJK.07/2020 Tahun 2020 Tentang Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan," *Ojk.Go.Id*, 2020, https://www.ojk.go.id/id/regulasi/Documents/Pages/Lembaga-Alternatif-Penyelesaian-Sengketa-Sektor-Jasa-Keuangan/pojk 61 - 07 - 2020.pdf.

[7] Agus Satory, "Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia," *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 2, no. 2 (2015): 269–90, https://doi.org/10.22304/pjih.v2n2.a4.

[8] Agus Satory et al., *Meneroka Relasi Hukum, Negara, Dan Budaya* (Yayasan Pustaka Obor Indonesia, 2017).

[9] OECD, *Prinsip Tata Kelola Perusahaan G20/OECD*, *Firstmedia*, 2018, http://www.firstmedia.co.id/corporate-governance/prinsip-tata-kelola-perusahaan.

[10] Verni Juita, Firdaus Firdaus, and Tria Najla Prima Hermanto, "Studi Prilaku Pengguna Layanan Financial Technology (Fintech) Di Indonesia: Analisa Persepsi Risiko Dan Manfaat," *Jurnal Inovasi Pendidikan Ekonomi (JIPE)* 10, no. 2 (2020): 118, https://doi.org/10.24036/011100040.

[11] Megawati Agus Cristine, Frangki Mario Angelo Risakota, and Steffy Ruth Celine Sirait, "Perlindungan Data Pribadi Dalam Sistem Skoring Kredit Otomatis Oleh Fintech Di Indonesia: Analisis Yuridis Normatif Berdasarkan Undang- Undang Nomor 27 Tahun 2022," *Jurnal Studi Hukum Modern* 4, no. 7 (2025), https://journalversa.com/s/index.php/jshm/article/view/860?utm_source=chatgpt.com.

[12] Pawel Drozdowski et al., "Demographic Bias in Biometrics: A Survey on an Emerging Challenge," *IEEE Transactions on Technology and Society* 1, no. 2 (2020): 89–103, https://doi.org/10.1109/tts.2020.2992344.

[13] Rina Arum Prastyanti, Rezi Rezi, and Istiyawati Rahayu, "Ethical Fintech Is a New Way of Banking," *Kontigensi : Jurnal Ilmiah Manajemen* 11, no. 1 (2023): 255–60, https://doi.org/10.56457/jimk.v11i1.353.

mempelajari aspek hukum perlindungan data, etika algoritma, dan tata kelola perusahaan (GCG) fintech di Indonesia. Oleh karena itu, penelitian ini memperbarui dengan menawarkan model tata kelola data fintech yang mengintegrasikan kerangka hukum, prinsip etik, dan prinsip AI.

Penelitian ini bertujuan mengkaji kerangka hukum positif perlindungan data fintech, merumuskan prinsip etika operasional seperti *fairness*, minimisasi data, dan *privacy by design/default*, serta menyusun model tata kelola data berbasis GCG dan three lines of defense beserta indikator kinerja. Manfaat penelitian mencakup kontribusi akademik pada literatur etika hukum GCG, panduan praktis bagi industri dalam desain e-KYC dan pengendalian risiko, masukan regulatif untuk harmonisasi standar dan pengawasan berbasis risiko, serta manfaat sosial berupa peningkatan literasi privasi, akses penyelesaian sengketa seperti LAPS-SJK, dan penguatan kepercayaan publik.

## METODE PENELITIAN

Untuk mengevaluasi norma positif, asas, dan doktrin yang mengatur perlindungan data konsumen di perusahaan fintech, penelitian ini menggunakan pendekatan yuridis normatif yang terdiri dari hasil deskriptif-analitis dan preskriptif. Selanjutnya, temuan ini dimasukkan ke dalam kerangka Etika Hukum Tata Kelola (EHT). Untuk melakukan analisis, digunakan pendekatan perundang-undangan, konseptual, perbandingan, dan kasus selektif. UU PDP 2022, bersama dengan peraturan turunan dan POJK terkait, dikaji dan dibandingkan dengan standar internasional seperti GDPR, CCPA, PDPA, dan APEC. Bahan hukum tersier terdiri dari literatur akademik dan laporan industri, relevansi, dan kemutakhiran, dan bahan primer terdiri dari peraturan perundang-undangan dan pedoman otoritas[14]. Bahan dikumpulkan melalui penelitian kepustakaan dan pemeriksaan dokumen yang dipetakan secara sistematis dalam lembar ekstraksi. Analisis kualitatif mencakup penafsiran hukum, klasifikasi norma, analisis konten kontrak baku dan kebijakan privasi, analisis perbedaan antara praktik domestik dan standar internasional, dan sintesis preskriptif menjadi kerangka EHT dan indikator kinerja tata kelola data. Pemetaan norma, identifikasi risiko proses, komparasi standar, penilaian perbedaan, dan pembuatan rubrik kematangan pemerintah adalah semua langkah dalam proses penelitian. Penelitian ini dibatasi oleh sifat normatif-doktrinal, kecepatan regulasi, dan keterbatasan untuk mendapatkan dokumen internal dari pelaku industri.

## HASIL DAN PEMBAHASAN

### Pemetaan Kewajiban Hukum Fintech Terkait Perlindungan Data Konsumen

#### Kewajiban Umum menurut UU PDP

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menempatkan penyelenggara fintech dalam kapasitasnya sebagai Pengendali dan/atau Pemroses pada sejumlah kewajiban kunci sepanjang siklus hidup data (pengumpulan pemrosesan penyimpanan transfer penghapusan):

a. dasar pemrosesan yang sah (*consent*, kontrak, kewajiban hukum, kepentingan vital, kepentingan umum, kepentingan sah)
b. pemberitahuan yang jelas terkait tujuan, kategori data, jangka retensi, penerima data
c. prinsip minimisasi dan pembatasan tujuan
d. keamanan data yang proporsional terhadap risiko
e. pemenuhan hak subjek data (akses, koreksi, hapus, tarik persetujuan, keberatan atas pemrosesan, portabilitas data sepanjang diatur)
f. pemberitahuan insiden kebocoran data kepada otoritas/ subjek data
g. pengawasan internal termasuk fungsi yang menjalankan kewajiban perlindungan data.

Implikasi praktisnya: fintech perlu memiliki Register Kegiatan Pemrosesan (RoPA), Kebijakan Retensi, Prosedur Insiden & Pemberitahuan, Penilaian Dampak Privasi (DPIA/PIA) untuk proses berisiko tinggi (mis. biometrik dan profiling keputusan otomatis), serta mekanisme verifikasi identitas untuk memenuhi hak subjek data.

---

[14] OECD, *G20/OECD Principles of Corporate Governance*, *OECD Publishing*, vol. N/A, 2023, https://www.oecd.org/en/publications/g20-oecd-principles-of-corporate-governance-2023_ed750b30-en.html; Ohnny Ibrahim, *Teori Dan Metodologi Penelitian Hukum Normatif* (Bayumedia, 2006); Peter M. Marzuki, *Penelitian Hukum: Edisi Revisi* (Kencana Prenada Media, 2005).

**Kewajiban Sektoral OJK**

Berbagai POJK yang saling melengkapi mengatur kewajiban sektoral OJK dalam hal perlindungan data dan operasi fintech. Tata kelola, manajemen risiko, kesehatan penyelenggara, kecukupan ekuitas, pengelolaan unit usaha syariah, dan kewajiban perlindungan konsumen, termasuk keamanan TI, kelangsungan bisnis, dan pemisahan fungsi pengendalian, diatur dalam POJK 40/2024. Sebaliknya, POJK 8/2023 tentang APU PPT mewajibkan proses identifikasi, verifikasi, dan pemantauan berkelanjutan terhadap pelanggan. Proses ini termasuk verifikasi non-tatap muka melalui e-KYC, penilaian risiko berbasis profil risiko, *screening* daftar terlarang, dan pemantauan dan pelaporan terus menerus. Kegagalan kontrol dapat menyebabkan risiko penipuan identitas dan sanksi kepatuhan. Dalam hal desain persetujuan dan mekanisme penagihan yang etis dalam fintech, POJK 6/2022 jo. 22/2023 menetapkan standar perlindungan konsumen seperti keterbukaan informasi, penanganan pengaduan, dan larangan praktik menyesatkan atau tidak adil. Selain itu, POJK 61/2020 menetapkan LAPS SJK sebagai metode penyelesaian sengketa non-litigasi dan harus dimasukkan ke dalam sistem penyelesaian sengketa internal perusahaan. Terakhir, POJK 3/2024 tentang Sandbox dan Inovasi Teknologi Sektor Keuangan (ITSK) memastikan bahwa semua inovasi, termasuk identitas digital, diuji untuk kepatuhan dan risiko sebelum dijual secara luas.

**Ranah Hukum Privat: Perjanjian Baku**

Kontrak baku (ToS, *Privacy Policy*, *Consent Form*) harus menghindari klausul tidak adil, *bundled consent*, tujuan pemrosesan yang kabur, dan retensi berlebih. Doktrin dan studi hukum konsumen Indonesia menegaskan dampak asimetri informasi dan posisi tawar yang timpang pada sektor jasa keuangan; ini menuntut keterbacaan dan opsi yang bermakna bagi konsumen.

**Integrasi Etika ke Dalam Desain Produk & Proses**

**Prinsip-Prinsip Etis Operasional**

Prinsip etis operasional untuk perlindungan data perusahaan fintech terdiri dari beberapa dasar yang harus dimasukkan ke dalam kebijakan dan praktik sehari-hari. Pertama, keadilan, keadilan, dan transparansi: pemrosesan data harus memiliki dasar hukum yang jelas, dilakukan secara adil bagi subjek data, dan terbuka untuk semua orang. Ini termasuk penjelasan tentang tujuan pemrosesan, hak pengguna, dan larangan praktik manipulatif atau pola gelap yang menyesatkan. Kedua, pengurangan dan pembatasan tujuan data mewajibkan pengumpulan dan penyimpanan hanya data yang benar-benar diperlukan untuk tujuan tertentu yang sah. Ada juga batasan waktu retensi yang proporsional dan mekanisme untuk menghapus data saat tidak lagi relevan. Ketiga,*privacy by design/default* memerlukan pengembangan kontrol privasi dan keamanan dari tahap konsep hingga penggunaan. Ini termasuk penggunaan arsitektur yang meminimalkan eksposur data, enkripsi, dan pseudonimisasi, serta pengaturan *default* yang paling aman bagi pengguna. Keempat, *non-discrimination & fairness* mewajibkan uji bias pada model skor, profil risiko, dan sistem deteksi penipuan baik sebelum penerapan maupun secara berkelanjutan. Mereka juga mewajibkan penyesuaian desain jika terjadi ketidakadilan yang berdampak pada kelompok rentan. Kelima, kemampuan untuk menjelaskan dan menentang memastikan bahwa keputusan otomatis tidak bersifat "kotak hitam" yang tidak dapat diakses. Perusahaan harus dapat menjelaskan logika pengambilan keputusan yang relevan bagi pengguna dan menyediakan jalur untuk keberatan, eskalasi, atau intervensi manusia dalam kasus di mana pengguna merasa dirugikan. Secara keseluruhan, prinsip-prinsip ini bukan hanya standar etika normatif, melainkan pedoman operasional yang harus diukur melalui kebijakan, kontrol teknis, pelatihan staf, dan indikator kinerja untuk menjamin perlindungan data yang efektif dan berkelanjutan.

**Etika e-KYC dan *Automated Decisioning***

Perusahaan fintech harus memastikan bahwa proses identifikasi digital dan penilaian otomatis berlangsung secara adil, akuntabel, dan aman sesuai dengan aturan e-KYC dan proses pengambilan keputusan otomatis. Untuk mengidentifikasi kemungkinan bias pada model verifikasi dan penilaian risiko, uji *fairness* harus dilakukan dengan menggunakan metrik kuantitatif seperti perbedaan kesempatan yang sama dan perbandingan dampak yang berbeda. Untuk memberikan penjelasan kepada pengguna dan auditor, dokumentasi teknis seperti garis data, nilai fitur, dan alasan penolakan harus disusun dengan jelas. Selain itu, kontrol *liveness* dan anti-*Deepfake* harus dirancang secara menyeluruh, termasuk deteksi *spoofing*, respons tantangan, analisis sinyal perangkat, dan korelasi perilaku

pengguna. Dalam kasus berisiko tinggi, pengawasan manusia harus ditambahkan untuk mencegah kesalahan verifikasi. Untuk menangani kasus edge, pendekatan *human-in-the-loop* menjadi penting karena memungkinkan analis kepatuhan untuk mengoverride keputusan otomatis ketika ditemukan anomali yang signifikan. Terakhir, pengelolaan retensi data harus ketat: data biometrik harus dipisahkan, dilindungi dalam template terenkripsi, dan pembatasan akses, dan dihapus setelah tujuan pemrosesan selesai. Praktik-praktik ini memastikan bahwa e-KYC dan pengambilan keputusan automatis tidak hanya efektif tetapi juga sesuai dengan etika, perlindungan data, dan tata kelola yang baik.

**Etika Penagihan**

Dalam industri fintech, etika penagihan membutuhkan standar perilaku yang ketat agar hubungan dengan pelanggan tetap manusiawi, proporsional, dan bebas dari praktik penyalahgunaan. *Code of Conduct* harus secara tegas melarang intimidasi, pelecehan, ancaman, *doxing*, dan penggunaan data kontak darurat yang berlebihan yang tidak terkait dengan kewajiban pembayaran. Kewajiban sertifikasi, pelatihan berkala, dan mekanisme pemantauan yang menggunakan rekaman interaksi untuk memastikan kepatuhan terhadap standar perilaku menjaga profesionalisme penagih. Untuk menjaga integritas proses penagihan dan memberikan efek jera, pelanggaran harus dikenai sanksi bertingkat. Selain itu, konsumen harus diberitahu secara akurat tentang saldo, kewajiban, dan status pembayaran melalui kanal resmi, pada waktu yang tepat. Prinsip-prinsip etis ini melindungi konsumen dan memperkuat bisnis fintech.

**Desain Tata Kelola (GCG) dan Model Operasi**
**Struktur dan Peran**

Dalam perusahaan fintech, struktur tata kelola perlindungan data mengharuskan peran yang jelas dan akuntabel di seluruh lapisan organisasi. Di antara tanggung jawab strategis mereka, Dewan Komisaris dan Direksi menetapkan kebutuhan risiko, mengesahkan kebijakan privasi dan keamanan informasi, dan mengawasi indikator kinerja penting yang menunjukkan seberapa baik tata kelola data. Komite Risiko dan Komite Teknologi/Keamanan menjalankan pengawasan operasional yang lebih teknis. Komite Teknologi/Keamanan berfungsi sebagai forum evaluasi berkala tentang risiko data, model, dan keamanan siber. Pada tingkat fungsional, seorang Pelindung Data (DPO) atau unit setara harus independen, memiliki akses langsung ke dewan, dan diizinkan untuk memberikan tanda tangan terhadap kebijakan pengelolaan data dan Evaluasi Efek Pelindung Data (DPIA). Mekanisme Tiga Lini Pertahanan memperkuat arsitektur ini. Lini pertama, yang terdiri dari produk, operasi, dan TI, bertanggung jawab atas pelaksanaan kontrol harian; lini kedua, yang terdiri dari kepatuhan dan manajemen risiko, membuat kebijakan, melakukan pengawasan, dan pelatihan; dan lini ketiga, yang terdiri dari audit internal, secara mandiri memberikan jaminan dan memastikan tindak lanjut atas setiap hasil audit. Struktur ini memastikan tata kelola data yang lengkap, dapat diukur, dan dapat dipertanggungjawabkan.

**Proses Kunci dan Artefak**

Dalam perusahaan fintech, pengelolaan perlindungan data harus didukung oleh sejumlah prosedur penting dan elemen tata kelola yang terdokumentasi dengan baik. Perusahaan harus memiliki catalog data, sistem klasifikasi dan tagging untuk data sensitif dan biometrik, *Record of Processing Activities* (RoPA), dan kebijakan retensi dan pemusnahan data yang aman dalam domain manajemen data. Model manajemen mengelola risiko pada sistem penilaian otomatis. Model manajemen mencakup inventarisasi model, proses validasi, pengujian keadilan, pengendalian perubahan, dan validasi berkala. Vendor manajemen memperkuat hubungan dengan pihak ketiga dengan mewajibkan tindakan keamanan, lokasi penyimpanan data, dan *sub-processor*. Ini juga disertai dengan klausul *Data Processing Agreement* (DPA), SLA/SLO yang terukur, hak audit, dan pengawasan terus menerus. API manajemen memastikan keamanan integrasi layanan; ini menetapkan batas tingkat, ruang lingkup akses, keamanan token, dan manajemen rahasia, serta melakukan pengujian potensi penyalahgunaan. Untuk menangani insiden, organisasi harus memiliki playbook respons terhadap insiden yang mencakup skenario kebocoran data, latihan di atas meja, matriks pemberitahuan kepada otoritas dan subjek data, dan review *pasca-incident* yang berorientasi perbaikan. Seluruhnya dilengkapi dengan

program pelatihan dan peningkatan pengetahuan yang berjenjang, mulai dari pelatihan awal hingga pelatihan tahunan, dan modul khusus untuk posisi seperti analis risiko, penagih, atau pengembang.

**Indikator Kinerja (KPI) & Ambang Pengendalian**

**KPI Kepatuhan & Tata Kelola**

Kepatuhan terhadap kewajiban penilaian dampak perlindungan data (DPIA), yang diukur dari jumlah proses berisiko tinggi yang memiliki DPIA dibandingkan dengan total proses berisiko tinggi, dengan sasaran capaian penuh atau 100%, juga merupakan indikator penting untuk tingkat pemenuhan hak subjek data. Memanfaatkan metrik kepatuhan vendor untuk mengukur jumlah pelanggaran SLA yang terjadi dibandingkan dengan total vendor material, kinerja pihak ketiga diprioritaskan. Targetnya adalah tidak ada pelanggaran yang signifikan pada setiap kuartal.

**KPI Operasional & Risiko**

KPI operasional dan risiko adalah alat pemantauan kinerja yang menunjukkan seberapa baik organisasi mengelola insiden, menjaga kualitas kontrol, dan menjaga konsumen aman. Untuk menilai kecepatan deteksi dan pemulihan, metrik MTTD/MTTR untuk insiden data, yang diukur dalam hari atau jam, sangat penting. Dengan target penurunan dari kuartal ke kuartal. Tingkat insiden per 100 ribu akun aktif juga digunakan untuk menilai stabilitas operasional, dan diharapkan tetap berada di bawah standar industri internal. Dalam proses e-KYC, tingkat *false positive* dan *false negative*, yang ditetapkan dalam rentang ketat, dipantau juga oleh sistem identitas digital. Tingkat ini langsung terkait dengan keinginan risiko organisasi. Untuk melindungi konsumen, tingkat keluhan pengembalian hutang dihitung berdasarkan rasio keluhan yang sah terhadap jumlah akun yang ditagih; tingkat ini ditargetkan untuk menurun setiap kuartal. Meskipun demikian, *Fairness* Delta menggunakan perbedaan kesempatan yang sama untuk mengevaluasi elemen keadilan model. Ini harus tetap berada di bawah ambang toleransi tertentu ($\leq$ x%). Indikator gabungan ini menunjukkan kesehatan operasional, integritas proses, dan komitmen perusahaan terhadap praktik yang aman dan etis.

***Leading Indicators***

*Indicator* utama berkonsentrasi pada kesiapan dan ketahanan sistem melalui berbagai metrik penting. Untuk memastikan bahwa seluruh pengembang dan staf yang terkait memiliki kompetensi yang memadai, tingkat penyelesaian pelatihan *coding* aman dan privasi sangat penting, dengan target kepatuhan minimal 98%. Selain itu, *patch latency* untuk kerentanan kritis dipantau secara ketat, dengan latency yang ditetapkan tidak lebih dari tujuh hari untuk mengurangi risiko eksploitasi. Selain itu, cakupan pemantauan sangat penting untuk mendeteksi insiden secara proaktif. Ini diukur melalui ketersediaan sinyal dan telemetri pada seluruh sistem material, dengan target *coverage* seratus persen. Secara keseluruhan, sinyal-sinyal ini berfungsi sebagai sinyal awal terhadap potensi risiko keamanan dan privasi sebelum menjadi insiden yang lebih besar.

***Case-Based Reasoning*: Penerapan Kerangka EHT**

Kasus A: Insiden e-KYC dan *Deepfake* menunjukkan bagaimana akun baru dapat melewati verifikasi *liveness* melalui video sintetis. Penyelenggara fintech harus menggunakan *liveness* multi-faktor, seperti deteksi gerak mikro, tanggapan tantangan-tanggapan acak, korelasi sinyal perangkat, dan verifikasi dokumen berbasis MRZ/PKD dan pengujian kecepatan. Dalam kasus anomali tinggi, eskalasi manusia masih diperlukan. Secara etika, perusahaan harus menerapkan minimisasi dan retensi data biometrik, menyediakan jalur banding, dan memberikan alasan yang transparan untuk menolak. Untuk memastikan sistem identitas digital tetap aman, model manajemen, pengujian tim merah berkala, dan laporan ke komite risiko adalah hal penting.

Kasus B: Penagihan Tidak Etis oleh Vendor Pihak Ketiga Masalah muncul ketika vendor penagihan mengancam kontak darurat, melanggar etika dan perlindungan data. Kontrol yang diperlukan termasuk kode tindakan yang tegas, sertifikasi petugas penagihan, whitelisting kanal komunikasi resmi, rekaman panggilan, audit lokasi, dan aturan dua strikes. Dari sudut pandang etika-hukum, Anda bertanggung jawab untuk mencegah penyalahgunaan, pelecehan, atau penyalahgunaan data kontak serta memberikan permintaan maaf atau kompensasi yang wajar kepada pelanggan. Dalam tata kelola, SLA, DPA, hak audit, mekanisme *offboarding* vendor bermasalah, dan pelaporan kepada Lini 2 dan Lini 3 meningkatkan otoritas vendor.

Kasus C: Kesalahan konfigurasi *cloud*, seperti *bucket* penyimpanan, menyebabkan kebocoran data PII. Pengawasannya mencakup penerapan infrastruktur *as code* dengan peraturan *as code*, penggunaan CSPM/CIEM untuk mendeteksi konfigurasi berisiko, enkripsi data saat istirahat dan saat dalam perjalanan, dan rotasi berkala untuk rahasia. Secara etika dan hukum, perusahaan harus melaporkan insiden sesuai dengan UU PDP dan menawarkan dukungan untuk mitigasi, seperti melacak kredit konsumen yang terdampak. Untuk mencegah kejadian serupa dan meningkatkan ketahanan data, penyelenggara tata kelola harus melakukan *review* pasca-kejadian, menemukan akar masalah, meningkatkan kontrol internal, dan meningkatkan pelatihan tim.

**Peta Jalan Implementasi (12 Bulan)**

Peta jalan implementasi selama dua belas bulan bertujuan untuk secara bertahap namun terukur membangun fondasi untuk tata kelola data, model, dan risiko teknologi. Pada tahap 0 90 hari *(quick wins)*, fokus diarahkan pada pembentukan dasar operasional melalui kegiatan seperti pemetaan data dan penyusunan RoPA, penetapan kebijakan retensi, dan pembuatan *playbook* insiden untuk respons kebocoran. Sementara kode perilaku penagihan dibuat untuk perilaku operasional, vendor register dan DPA standar dibuat untuk meningkatkan pengelolaan pihak ketiga. Untuk memastikan bahwa developer, penagih, dan analis siap sejak awal, pelatihan wajib diperlukan untuk peran kritis ini. Dalam waktu 3 hingga 6 bulan, organisasi mulai melakukan hal-hal yang lebih kompleks, seperti menerapkan DPIA untuk semua proses berisiko tinggi, seperti biometrik dan penghitungan, dan menerapkan pengujian *fairness* sebelum model digunakan di produksi. Implementasi CSPM/CIEM dan latihan *table-top* untuk kesiapsiagaan insiden meningkatkan kontrol teknologi. Pada tahap ini, *notice privacy* baru yang lebih mudah dipahami dibuat dan kanal keluhan pengguna ditambahkan ke mekanisme LAPS SJK. Pada tahap 6 12 bulan, pemerintahan dikuatkan secara menyeluruh. Ini termasuk membentuk komite risiko dan teknologi, menerapkan model pemerintahan sepenuhnya (termasuk inventaris, validasi, dan re-validasi), menerbitkan laporan transparansi tahunan, dan membangun sistem pemantauan terus-menerus bagi pihak ketiga. Penyusunan *maturity rubric* sebagai acuan peningkatan berkelanjutan dan audit internal tematik ditutup rangkaian ini.

**Implikasi Kebijakan**

Semua pemangku kepentingan harus berpartisipasi secara aktif ketika kerangka pelindungan data diterapkan pada perusahaan fintech. Dibutuhkan panduan teknis yang lebih operasional dari regulator dan asosiasi industri, terutama yang berkaitan dengan penilaian *fairness* pada model kredit dan deteksi fraud, kerangka model manajemen risiko yang seragam, tolok ukur notifikasi insiden, dan standar layanan penyelesaian sengketa melalui LAPS SJK. Dari sisi industri, perusahaan harus mengadopsi prinsip *privacy engineering* dan secure-by-*default* sebagai standar minimum dalam perancangan sistem, disertai dengan standar penyelesaian sengketa melalui LAPS SJK. Untuk menjamin hak dan perlindungan konsumen, peningkatan literasi privasi dan akses ke kanal pengaduan yang terintegrasi dengan mekanisme penyelesaian sengketa alternatif (ADR) sangat penting.

Hasil analisis menunjukkan bahwa praktik perlindungan data fintech, seperti e-KYC, algoritma keadilan, etika penagihan, dan tata kelola risiko, sejalan dengan teori privasi Westin tentang kendali individu atas data serta prinsip FIPPs (keadilan, keadilan, transparansi, pengurangan data, dan tanggung jawab). Perlindungan yang diatur dalam UU PDP dan POJK terkait dijamin melalui penerapan DPIA, retensi terbatas, kontrol anti-*Deepfake*, dan mekanisme banding. Teori etika bisnis Velasquez dan penelitian Satory tentang lemahnya posisi konsumen dalam kontrak baku diperkuat oleh temuan tentang risiko diskriminasi algoritmik, pola gelap, dan penagihan tidak etis[15]. Proses seperti *human-in-the-loop, whitelisting channel*, dan *code of conduct* menunjukkan penerapan prinsip keadilan dan *non-maleficence* dalam operasi fintech. Secara keseluruhan, hasil penelitian menunjukkan bahwa penerapan hukum, etika, dan tata kelola dalam kerangka konseptual menentukan keberhasilan perlindungan data fintech. Ini ditunjukkan oleh penggunaan tiga lini pertahanan, peran DPO, komite risiko, dan pemenuhan KPI seperti DPIA dan MTTD/MTTR.

Hasil penelitian menunjukkan bahwa, terutama dalam hal transparansi, akuntabilitas, dan pengelolaan risiko teknologi, perlindungan konsumen dan tata kelola data fintech masih menantang.

[15] Marzuki, *Penelitian Hukum: Edisi Revisi*; Satory, "Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia."

Hasil ini sejalan dengan Satory [16], yang menyatakan bahwa ketidakseimbangan posisi tawar menyebabkan kontrak baku sering merugikan konsumen. Ini terbukti dalam praktik layanan fintech yang masih kekurangan penjelasan jelas tentang pemrosesan data. Hasil ini juga sejalan dengan pendapat Mihradi & Mahayana bahwa perubahan budaya hukum dan tata kelola internal perusahaan memerlukan lebih dari regulasi [17].

Selain itu, hasil penelitian mendukung laporan OECD yang menekankan bahwa kepemimpinan sangat penting untuk menumbuhkan kepercayaan publik. Ini berhubungan dengan penelitian fintech di Indonesia yang menunjukkan bahwa masalah keamanan data dan privasi masih menjadi kendala utama dalam adopsi. Penelitian normatif tentang sistem skoring otomatis juga menunjukkan bahwa UU PDP masih kurang dilaksanakan, terutama dalam hal transparansi, tujuan, dan hak keberatan pemilik data.

Hasil penelitian ini juga didukung oleh penelitian yang dilakukan di seluruh dunia tentang etika AI dan bias algoritmik. Untuk mengurangi risiko diskriminasi yang disebabkan oleh bias model pembelajaran mesin, diperlukan audit keadilan, sistem pengawasan, dan kontrol etis yang ketat. Persepsi risiko, etika fintech, atau tata kelola AI adalah komponen yang biasanya tidak dibahas dalam penelitian sebelumnya. Penelitian ini menawarkan cara yang lebih terintegrasi menghubungkan kerangka hukum, prinsip etika, dan keadilan algoritma untuk membuat model tata kelola data fintech yang lebih komprehensif untuk industri fintech Indonesia.

## KESIMPULAN

Studi ini menemukan bahwa perlindungan data fintech memiliki banyak aspek dan membutuhkan kerja sama etika, hukum, dan tata kelola agar inovasi seperti LPBBTI, dompet digital, dan e-KYC aman dan tidak terbatas pada kepatuhan administratif. Meskipun kerangka hukum Indonesia, terutama UU PDP dan berbagai POJK, cukup lengkap, masalah utama adalah konsistensi implementasi. Ini terutama berkaitan dengan pengelolaan risiko e-KYC, bias algoritmik, perjanjian baku, dan tata kelola internal, termasuk tugas dewan, tugas DPO, tiga lini pertahanan, dan pengawasan vendor. Untuk meningkatkan akuntabilitas, diperlukan metrik yang dapat diukur, mekanisme pemulihan yang efektif, dan kolaborasi antarlembaga.

Hasilnya menunjukkan bahwa regulasi harus menetapkan standar teknis *fairness* dan model risiko; DPIA harus bertanggung jawab atas proses berisiko tinggi; peningkatan sistem notifikasi insiden; dan peningkatan pengawasan pihak ketiga. Bagi industri, teknologi privasi, model pemerintahan, e-KYC berlapis, etika penagihan, kesiapan insiden, pelatihan, dan transparansi publik adalah hal-hal yang paling penting. Organisasi dan masyarakat diharapkan memberikan dukungan dengan menetapkan standar praktik, memahami privasi, dan menggunakan mekanisme pengaduan. Selain itu, penelitian ini menegaskan manfaat teoretis kerangka EHT sebagai model integratif dan membuka peluang untuk penelitian lebih lanjut tentang audit empiris, penilaian keadilan, tata kelola data lintas batas, biaya-manfaat teknik privacy, dan ADR.

## DAFTAR PUSTAKA

Andrea, Jenny, Yaswirman, and Rembrandt. “Akibat Hukum Penundaan Pengikatan Jaminan Dalam Perjanjian Kredit Modal Kerja Pt. Bank Negara Indonesia (Persero) Tbk.” *Van Java Law Journal* 1, no. 01 (2024): 50–79. https://doi.org/10.64578/vjlj.v1i01.72.

Asosiasi Fintech Pendanaan Bersama Indonesia. “Pedoman Perilaku Pemberian Layanan Pendanaan Bersama Berbasis Teknologi Informasi Secara Bertanggung Jawab,” no. November (2023): 1–15. https://afpi.or.id/assets/document/Pedoman_Perilaku_AFPI_2023_Clean.pdf.

CNN Indonesia. “Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual.” *CNN Indonesia*, 2020. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

Cristine, Megawati Agus, Frangki Mario Angelo Risakota, and Steffy Ruth Celine Sirait. “Perlindungan Data Pribadi Dalam Sistem Skoring Kredit Otomatis Oleh Fintech Di Indonesia: Analisis Yuridis Normatif Berdasarkan Undang- Undang Nomor 27 Tahun 2022.” *Jurnal Studi Hukum Modern* 4, no.



(2025).

[16] Satory, “Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia.”

[17] Satory et al., *Meneroka Relasi Hukum, Negara, Dan Budaya*.

https://journalversa.com/s/index.php/jshm/article/view/860?utm_source=chatgpt.com.

Dewan Komisioner OJK. "Otoritas Jasa Keuangan Republik Indonesia," 2015.

Drozdowski, Pawel, Christian Rathgeb, Antitza Dantcheva, Naser Damer, and Christoph Busch. "Demographic Bias in Biometrics: A Survey on an Emerging Challenge." *IEEE Transactions on Technology and Society* 1, no. 2 (2020): 89–103. https://doi.org/10.1109/tts.2020.2992344.

Ibrahim, Ohnny. *Teori Dan Metodologi Penelitian Hukum Normatif*. Bayumedia, 2006.

Juita, Verni, Firdaus Firdaus, and Tria Najla Prima Hermanto. "Studi Prilaku Pengguna Layanan Financial Technology (Fintech) Di Indonesia: Analisa Persepsi Risiko Dan Manfaat." *Jurnal Inovasi Pendidikan Ekonomi (JIPE)* 10, no. 2 (2020): 118. https://doi.org/10.24036/011100040.

Marzuki, Peter M. *Penelitian Hukum: Edisi Revisi*. Kencana Prenada Media, 2005.

Mita, F, A. "Pedoman Umum Governansi Korporat Indonesia (PUGKI) 2021." *Komite Nasional Kebijakan Governansi*, 2021, 37. https://knkg.or.id/wp-content/uploads/2022/06/PUGKI-2021-LORES.pdf.

OECD. *G20/OECD Principles of Corporate Governance*. *OECD Publishing*. Vol. N/A, 2023. https://www.oecd.org/en/publications/g20-oecd-principles-of-corporate-governance-2023_ed750b30-en.html.

———. *Prinsip Tata Kelola Perusahaan G20/OECD*. *Firstmedia*, 2018. http://www.firstmedia.co.id/corporate-governance/prinsip-tata-kelola-perusahaan.

OJK. "Peraturan Otoritas Jasa Keuangan Nomor 61/POJK.07/2020 Tahun 2020 Tentang Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan." *Ojk.Go.Id*, 2020. https://www.ojk.go.id/id/regulasi/Documents/Pages/Lembaga-Alternatif-Penyelesaian-Sengketa-Sektor-Jasa-Keuangan/pojk 61 - 07 - 2020.pdf.

Otoritas Jasa Keuangan. "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10 /Pojk.05/2022 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi," no. 184 (2014): 1–27.

———. "Pojk 40/2024," 2024, 1–23. https://ojk.go.id/id/regulasi/Pages/POJK-40-Tahun-2024-Layanan-Pendanaan-Bersama-Berbasis-Teknologi-Informasi.aspx.

Peraturan Otoritas Jasa Keuangan. "Peraturan Otorisasi Jasa Keuangan Republik Indonesia Nomor 3 Tahun 2024 Tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan." *Peraturan Otoritas Jasa Keuangan*, 2024.

Peraturan Pemerintah. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara RI (2019).

———. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Lembaran Negara RI (2019).

———. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara RI (2022).

Prastyanti, Rina Arum, Rezi Rezi, and Istiyawati Rahayu. "Ethical Fintech Is a New Way of Banking." *Kontigensi : Jurnal Ilmiah Manajemen* 11, no. 1 (2023): 255–60. https://doi.org/10.56457/jimk.v11i1.353.

Satory, Agus. "Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 2, no. 2 (2015): 269–90. https://doi.org/10.22304/pjih.v2n2.a4.

Satory, Agus, Ari Wuisang, Asmak Ul Hosnah, Isep H. Insan, Iwan Darmawan, I Wayan Suparta, Nazaruddin Lathif Mahipal, R. Muhammad Mihradi, and Sapto Handoyo D.P. *Meneroka Relasi Hukum, Negara, Dan Budaya*. Yayasan Pustaka Obor Indonesia, 2017.

Tempo.Co. "Data KTP Hingga Rekam Medis 2 Juta Nasabah BRI Life Diduga Bocor Dan Dijual." *Tempo.Co*, 2021. tempo.co/ekonomi/data-ktp-hingga-rekam-medis-2-juta-nasabah-bri-life-diduga-bocor-dan-dijual-490216#google_vignette.