Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No.4, Tahun 2026
doi.org/10.63822/8cb1qq25
Hal. 9186-9194

Perlindungan Data Nasabah dalam Era Digital: Tinjauan dari Kasus Kebocoran Data Bank DKI

Hambali H
Ilmu Hukum, Fakultas Hukum, Universitas Halu Oleo, Kota Kendari, Indonesia

*Email Korespodensi: hambalihusaini@uho.ac.id

Sejarah Artikel:

Diterima 27-07-2026
Disetujui 30-07-2026
Diterbitkan 31-07-2026

ABSTRACT

The rapid development of digital technology has fundamentally transformed the banking industry landscape, creating new challenges in customer data protection. This study aims to analyze the customer data protection challenges in the digital banking era through a case study of the Bank DKI data breach incident in 2025, examine the applicable legal framework, and formulate solutions to strengthen banking secrecy and public trust. The method used is normative legal research with statutory and conceptual approaches. The results show that the Bank DKI incident revealed systemic vulnerabilities in three key aspects: technical infrastructure, internal procedures, and human resources. The breach involved a third party allegedly colluding with internal management to access the system through high-level authorization, resulting in 807 anomalous transactions valued at Rp227.1 billion. The attack occurred through the BI-Fast payment system, with discrepancies between transaction records reaching Rp245.8 billion. Although the bank confirmed that customer funds and data remained secure, the incident highlighted a significant gap between existing regulations and on-the-ground implementation. This study finds that Law No. 27 of 2022 on Personal Data Protection has provided a strong legal foundation, but weak supervision and enforcement by regulators remain critical challenges. Responsive regulation, proactive supervision, and strengthening public legal literacy are urgently needed.

Keywords: *Customer data protection; digital banking; data breach; Bank DKI; cybersecurity; BI-Fast*

ABSTRAK

Perkembangan teknologi digital yang pesat telah mengubah lanskap industri perbankan secara fundamental, menghadirkan tantangan baru dalam perlindungan data nasabah. Penelitian ini bertujuan menganalisis tantangan perlindungan data nasabah di era perbankan digital melalui studi kasus insiden kebocoran data Bank DKI tahun 2025, mengkaji kerangka hukum yang berlaku, serta merumuskan solusi untuk memperkuat kerahasiaan bank dan kepercayaan masyarakat. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa insiden Bank DKI mengungkap kerentanan sistemik pada tiga aspek utama: infrastruktur teknis, prosedur internal, dan sumber daya manusia. Peretasan melibatkan pihak ketiga yang diduga bekerja sama dengan pihak internal manajemen untuk mengakses sistem melalui otorisasi tingkat tinggi, dengan 807 transaksi anomali senilai Rp227,1 miliar. Serangan terjadi melalui sistem pembayaran BI-Fast dengan selisih pencatatan transaksi mencapai Rp245,8 miliar. Meskipun bank menegaskan bahwa dana dan data nasabah tetap aman, insiden ini menyoroti kesenjangan signifikan antara regulasi yang ada dengan implementasi di lapangan. Penelitian ini menemukan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan hukum yang kuat, namun lemahnya pengawasan dan penegakan hukum oleh regulator masih

menjadi tantangan kritis. Diperlukan regulasi responsif, pengawasan proaktif, dan penguatan literasi hukum masyarakat.

Katakunci: Perlindungan data nasabah; perbankan digital; kebocoran data; Bank DKI; keamanan siber; BI-Fast

Bagaimana Cara Sitasi Artikel ini:

H, H. (2026). Perlindungan Data Nasabah dalam Era Digital: Tinjauan dari Kasus Kebocoran Data Bank DKI. Jejak Digital: Jurnal Ilmiah Multidisiplin, 2(4), 9186-9194. https://doi.org/10.63822/8cb1qq25

PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mengubah lanskap industri perbankan secara fundamental. Transformasi digital memungkinkan bank untuk menawarkan layanan yang lebih efisien dan mudah diakses melalui platform *online* dan aplikasi seluler. Di Indonesia, adopsi perbankan digital terus meningkat seiring dengan makin tingginya penetrasi internet dan penggunaan *smartphone*. Namun, di balik kemudahan ini, muncul tantangan baru yang signifikan, terutama terkait dengan keamanan data nasabah. Data pribadi dan finansial nasabah kini menjadi aset yang sangat berharga dan rentan terhadap ancaman siber, seperti peretasan dan kebocoran data.

Penelitian terdahulu menunjukkan bahwa insiden kebocoran data di sektor perbankan Indonesia sering disebabkan oleh kombinasi kerentanan sistem yang belum diperbarui dan kelalaian sumber daya manusia. Studi yang dilakukan oleh para peneliti menemukan bahwa 60% insiden kebocoran data pada lembaga perbankan di Indonesia disebabkan oleh faktor-faktor tersebut (Santoso, 2024). Kegagalan dalam penerapan protokol keamanan internal, seperti penggunaan kata sandi yang lemah dan kurangnya pelatihan karyawan, menjadi faktor signifikan dalam memudahkan serangan siber. Penelitian lain yang berfokus pada respons bank pasca-insiden kebocoran data menyimpulkan bahwa transparansi dan kecepatan komunikasi menjadi faktor kunci dalam memulihkan kepercayaan nasabah (Aminah, 2025).

Perbedaan penelitian ini dengan penelitian-penelitian sebelumnya terletak pada fokus analisisnya yang mengkaji secara mendalam kasus kebocoran data Bank DKI tahun 2025 sebagai studi kasus konkret, dengan mengaitkannya secara komprehensif pada kerangka regulasi yang berlaku di Indonesia, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta merumuskan solusi yang bersifat holistik mencakup aspek teknis, prosedural, dan kelembagaan. Penelitian ini juga menyoroti kelemahan sistemik pada infrastruktur pembayaran nasional BI-Fast yang menjadi celah utama serangan.

Prinsip dasar kerahasiaan bank yang diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan bertujuan untuk melindungi data nasabah. Akan tetapi, kerangka hukum tradisional ini belum sepenuhnya memadai untuk menghadapi kompleksitas ancaman siber di era digital. Isu kebocoran data nasabah menjadi perhatian serius karena tidak hanya merusak kepercayaan publik, tetapi juga dapat menimbulkan kerugian finansial dan risiko penyalahgunaan data.Kasus kebocoran data yang dialami oleh Bank DKI pada tahun 2025 menjadi salah satu contoh nyata betapa mendesaknya isu ini. Bank DKI diduga telah mengalami peretasan lebih dari satu kali sejak tahun 2024. Gangguan sistem yang terjadi sejak 29 Maret 2025 menyebabkan nasabah kesulitan mengakses layanan perbankan secara normal. Serangan siber terjadi melalui sistem pembayaran BI-Fast, mengakibatkan transaksi anomali pada rekening Bank DKI di Bank Negara Indonesia (BNI) yang digunakan sebagai rekening penyelesaian untuk layanan BI-Fast. Unit pengawasan Bank DKI mendeteksi penurunan drastis saldo BI-Fast antara pukul 11.00 dan 11.20 WIB, yang kemudian diikuti dengan aktivasi *panic button* pada pukul 11.36 WIB dan aktivasi *firewall* pada pukul 11.44 WIB.

Berdasarkan latar belakang tersebut, rumusan masalah yang akan dibahas dalam penelitian ini adalah: (1) Bagaimana kasus kebocoran data Bank DKI tahun 2025 mencerminkan tantangan perlindungan data nasabah di era digital? (2) Bagaimana regulasi perlindungan data nasabah yang berlaku di Indonesia dalam konteks perbankan digital? (3) Apa solusi untuk memperkuat kerahasiaan bank dan kepercayaan masyarakat pasca-insiden Bank DKI? Tujuan penelitian ini adalah untuk menganalisis kasus kebocoran data Bank DKI sebagai cerminan tantangan perlindungan data nasabah, mengulas regulasi yang berlaku, serta merumuskan solusi konkret untuk memperkuat kerahasiaan bank dan kepercayaan masyarakat.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*doctrinal legal research*) yang bertujuan untuk mengkaji norma-norma hukum yang mengatur perlindungan data nasabah di sektor perbankan serta mengidentifikasi kesenjangan antara *das sollen* dan *das sein* dalam praktik perlindungan data di era digital. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menelaah berbagai peraturan perundang-undangan yang relevan, serta pendekatan konseptual (*conceptual approach*) untuk mengkaji konsep-konsep hukum seperti kerahasiaan bank, perlindungan data pribadi, dan tanggung jawab hukum lembaga keuangan.

Bahan hukum primer yang digunakan meliputi Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum, serta POJK Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah.

Bahan hukum sekunder berupa laporan media mengenai insiden Bank DKI tahun 2025, hasil investigasi kepolisian dan PPATK, literatur hukum perbankan dan perlindungan data, serta jurnal ilmiah terkait. Analisis data dilakukan secara kualitatif dengan metode yuridis-normatif, yaitu menelaah asas, norma, dan ketentuan hukum positif kemudian menghubungkannya dengan permasalahan yang diteliti untuk menarik kesimpulan yang sistematis.

HASIL DAN PEMBAHASAN

Analisis Kasus Kebocoran Data Bank DKI Tahun 2025

Kasus kebocoran data Bank DKI pada tahun 2025 menjadi contoh krusial yang menyoroti kerentanan sektor perbankan di era digital. Gangguan sistem yang terjadi sejak 29 Maret 2025 menyebabkan nasabah kesulitan mengakses layanan perbankan secara normal, terutama melalui aplikasi JakOne Mobile. Bank DKI diduga telah mengalami peretasan lebih dari satu kali sejak tahun 2024. Peretasan terbesar dan paling signifikan terjadi pada 29 Maret 2025.

Kronologi dan Modus Operandi, Berdasarkan hasil investigasi kepolisian, serangan siber terjadi melalui sistem pembayaran BI-Fast. Peretasan mengakibatkan transaksi anomali pada rekening Bank DKI di Bank Negara Indonesia (BNI) yang digunakan sebagai rekening penyelesaian (*settlement account*) untuk layanan BI-Fast. Unit pengawasan Bank DKI mendeteksi penurunan drastis saldo BI-Fast antara pukul 11.00 dan 11.20 WIB. Pada pukul 11.36 WIB, mereka mengaktifkan sepenuhnya *panic button* untuk mencegah pencairan dana lebih lanjut, dengan *firewall panic button* diaktifkan pada pukul 11.44 WIB. Mereka menyadari penurunan saldo tidak berdasarkan perintah sah Bank DKI karena tidak ada catatan sistem atau pendebetan yang sesuai dalam sistem perbankan inti (*core banking system*). Namun, Artajasa sebagai penyedia infrastruktur BI-Fast telah memberi tahu mereka tentang adanya perintah transfer kredit dari Bank DKI.Sebanyak 807 transaksi anomali tercatat dengan nilai Rp227,1 miliar. Namun, sistem perbankan inti Bank DKI hanya mencatat Rp18,7 miliar, sementara catatan sistem menunjukkan transfer penyelesaian sebesar Rp245,8 miliar, menyoroti adanya selisih yang signifikan dalam pencatatan transaksi. Penetapan Tersangka dan Proses Hukum, Direktorat Tindak Pidana Siber Bareskrim Polri menetapkan

enam orang sebagai tersangka. Tiga tersangka—Rani Andriani, Erni Hidayat, dan Dudi Mangkudilaga—ditahan di Bandung, Jawa Barat. Tiga tersangka lainnya—M. Benny Ardiansyah, Zulfikar, dan Syafruddin—ditangkap di Medan, Sumatera Utara.

Menurut polisi, empat tersangka berperan membuat sarana transfer dana dan rekening penampung atas nama perusahaan fiktif, sekaligus membuka akun *mobile banking* serta dompet kripto untuk menyalurkan hasil pembobolan. Dua lainnya diduga membuat rekening penampung dana. Polisi masih memburu otak utama yang diduga menjadi pengendali serangan siber ini. Kepala PPATK Ivan Yustiavandana menyatakan pihaknya telah membekukan seluruh rekening yang digunakan pelaku untuk menampung dana hasil peretasan. Para tersangka dijerat dengan pasal berlapis: Pasal 46 ayat (1), Pasal 48 ayat (1), dan Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE); Pasal 80 ayat (2) dan Pasal 82 Undang-Undang Pengiriman Uang; Pasal 4, 5, dan 10 Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU); serta Pasal 363 KUHP tentang pencurian.

Pernyataan Bank DKI dan Pemerintah Provinsi Jakarta

Direktur Utama Bank DKI, Agus Haryoto Widodo, mengungkap adanya dugaan peretasan sistem bank yang menyebabkan kebocoran dana sejak 31 Maret 2025. Agus mengatakan peretasan melibatkan pihak ketiga yang diduga bekerja sama dengan sejumlah orang dari manajemen Bank DKI. "Yang jelas ada satu pihak ketiga yang tidak bekerja sebagaimana mestinya. Mereka menggunakan akses level tinggi untuk masuk ke sistem," kata Agus.

Agus menegaskan kebocoran hanya terjadi pada dana milik Bank DKI, bukan dana nasabah, dengan nilai kebocoran diperkirakan tidak lebih dari Rp100 miliar. Bank DKI telah melaporkan kasus ini ke Bareskrim Polri pada 1 April 2025.

Gubernur DKI Jakarta Pramono Anung menduga kuat adanya keterlibatan orang dalam dalam insiden ini. "Laporkan ke Bareskrim, proses hukum, karena ini sudah keterlaluan. Tidak mungkin, tidak melibatkan orang dalam," kata Pramono. Pramono memberhentikan Direktur Teknologi dan Operasional Bank DKI, Amirul Wicaksono, buntut gangguan layanan bank tersebut. "Kejadian di Bank DKI ini bukan pertama kali. Ini sudah ketiga kali dan kejadiannya hampir serupa," ucap Pramono.

Pramono juga menggandeng lembaga audit independen bertaraf internasional untuk mengusut tuntas dugaan kebocoran sistem di Bank DKI. Hasil audit forensik dan perbaikan sistem langsung dilakukan oleh lembaga yang ditunjuk Bank DKI. Layanan nasabah melalui kantor cabang dan ATM telah beroperasi normal sejak 7 April 2025.

Regulasi Perlindungan Data Nasabah pada Era Digital, Kerangka Hukum di Indonesia

Kerangka hukum perlindungan data di Indonesia telah mengalami evolusi signifikan. Landasan awalnya adalah UU Perbankan yang berfokus pada kerahasiaan simpanan. Kemudian, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mulai mengatur perlindungan data dalam konteks elektronik. Setiap penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia data pribadi. Tonggak penting adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP secara komprehensif mengatur hak-hak subjek data, kewajiban pengendali data, serta sanksi administratif dan pidana bagi pelanggar. Pasal 15 ayat (1) UU PDP menyatakan bahwa hak-hak subjek data pribadi dapat dikecualikan untuk kepentingan pertahanan dan keamanan nasional, proses penegakan hukum, kepentingan umum, serta pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan. Pasal 28 UU PDP menegaskan bahwa pengendali data pribadi wajib menjaga kerahasiaan data

pribadi.

Selain UU PDP, Otoritas Jasa Keuangan (OJK) memiliki peran krusial melalui berbagai peraturan. OJK telah menerbitkan Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum dan Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Melalui regulasi ini, OJK menempatkan keamanan siber dan tata kelola TI sebagai prasyarat daya saing industri perbankan.POJK Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah mengatur tata kelola TI, arsitektur sistem bagi layanan digital, kewajiban manajemen risiko TI, kepemilikan *Disaster Recovery Plan*, serta penempatan pusat data dan pusat pemulihan bencana di wilayah Indonesia. Bank penyelenggara Layanan Perbankan Elektronik atau Layanan Perbankan Digital wajib menerapkan prinsip perlindungan konsumen. Nasabah juga diwajibkan memberikan informasi yang benar, memperbarui data, serta memiliki itikad baik dalam hubungan dengan bank.

Kesenjangan Regulasi dan Implementasi

Kasus Bank DKI menunjukkan adanya kesenjangan signifikan antara regulasi dan implementasinya di lapangan. Meskipun UU PDP telah berlaku dan OJK telah menerbitkan berbagai peraturan terkait keamanan siber, penerapan sanksi dan pengawasan oleh regulator belum sepenuhnya efektif dalam mencegah insiden. Penelitian menunjukkan bahwa perlindungan hukum bagi nasabah telah diatur melalui berbagai undang-undang, namun efektivitasnya masih terbatas karena lemahnya pengawasan, kurangnya kepatuhan bank terhadap prinsip kehati-hatian, serta belum optimalnya mekanisme notifikasi dan pemulihan hak nasabah.

Kepala Eksekutif Pengawas Perbankan OJK, Dian Ediana Rae, menyatakan bahwa OJK telah mengingatkan bank pembangunan daerah (BPD) untuk senantiasa menerapkan manajemen risiko terkait TI sesuai dengan POJK serta SEOJK. Namun, gangguan di Bank DKI tetap terjadi dan disebabkan oleh lemahnya pengawasan sistem teknologi informasi yang berpotensi menyebabkan kebocoran data.
Kasus ini juga menyoroti adanya kelemahan pada infrastruktur sistem pembayaran nasional BI-Fast. Kelemahan pada sistem deteksi penipuan telah dieksploitasi oleh peretas untuk membobol bank, terutama bank kecil. Bank-bank daerah tidak memiliki sistem yang terhubung langsung ke BI-Fast, melainkan menggunakan *middleware* yang menjadi titik lemah dan sering menjadi target peretas. Selain itu, Bank Indonesia memiliki peran ganda sebagai operator sekaligus pengawas BI-Fast, yang menimbulkan pertanyaan tentang objektivitas pengawasan.

Tantangan Perlindungan Data Nasabah di Era Digital

Kasus Bank DKI merefleksikan dua tantangan utama dalam perlindungan data nasabah di era digital. *Pertama*, tantangan teknis dan infrastruktur. Komite Basel untuk Pengawasan Perbankan (BCBS) mendefinisikan risiko operasional sebagai risiko yang muncul akibat gagalnya suatu proses internal, manusia, sistem, atau adanya faktor peristiwa eksternal yang mengganggu kegiatan operasional. Meskipun Bank DKI diyakini telah memiliki infrastruktur keamanan, serangan siber berhasil menembus sistem pertahanan melalui celah pada sistem pembayaran BI-Fast. Spesialis Keamanan Teknologi Vaksincom, Alfons Tanujaya, menilai pembobolan tidak berasal dari sistem BI-Fast, melainkan dari sisi bank peserta melalui kompromi sistem internal bank.

Kedua, tantangan non-teknis dan prosedural. Kasus ini menyingkap kelemahan dari sisi non-teknis, termasuk kurangnya budaya keamanan di dalam organisasi dan prosedur penanganan data yang tidak ketat.

Peretasan melibatkan pihak ketiga yang diduga bekerja sama dengan manajemen Bank DKI menggunakan akses level tinggi. Hal ini menunjukkan bahwa teknologi tanpa sumber daya manusia yang terlatih dan prosedur yang disiplin tidak akan mampu menjamin keamanan data.
Bank-bank daerah tidak memiliki kapasitas untuk menerapkan sistem keamanan yang canggih karena investasi yang dibutuhkan signifikan. Mereka sering menjadi target peretas karena sistem keamanan yang lebih lemah dibandingkan bank besar.

Peran Otoritas Jasa Keuangan dan Tindak Lanjut Regulasi

Menanggapi insiden ini, OJK mengambil sejumlah langkah strategis. OJK melakukan *crash program* pemeriksaan terhadap seluruh BPD di Indonesia dengan fokus pada ketahanan dan keamanan siber. Penguatan dilakukan melalui regulasi TI, manajemen risiko, dan pencegahan *fraud* serta transaksi anomali. OJK memberikan peringatan keras kepada Bank DKI terkait gangguan sistem IT. Bank DKI diminta untuk meningkatkan proses digitalisasi dengan penguatan sistem IT perbankan guna memitigasi insiden serangan siber. OJK menekankan bahwa peningkatan proses digitalisasi di sektor jasa keuangan harus diimbangi dengan penguatan sistem TI perbankan, sehingga bank dapat memitigasi insiden TI yang berpotensi mengganggu operasional, merusak reputasi Pelaku Usaha Sektor Keuangan (PUSK), serta mengancam stabilitas sistem keuangan secara keseluruhan.

OJK juga menekankan pentingnya peran aktif dari seluruh PUSK melalui *Chief Information Security Officer* untuk menjaga operasional bisnis yang aman serta responsif dalam pencegahan dan pengamanan seluruh Infrastruktur Informasi Vital di masing-masing Lembaga Jasa Keuangan. OJK senantiasa bersinergi dan berkolaborasi dengan PUSK, otoritas, dan aparat penegak hukum untuk menciptakan ekosistem sistem TI perbankan dan keamanan siber yang tangguh. Berbagi informasi, pengalaman, dan praktik terbaik menjadi langkah strategis dalam mengidentifikasi potensi ancaman, merespons insiden dengan lebih cepat, dan mencegah risiko yang lebih besar.

Solusi Memperkuat Kerahasiaan Bank dan Kepercayaan Masyarakat

Untuk memulihkan kepercayaan masyarakat dan mencegah terulangnya insiden serupa, diperlukan solusi yang komprehensif dan terkoordinasi.
Pertama, solusi teknis dan operasional. Bank harus mengadopsi pendekatan pertahanan berlapis (*defense-in-depth*). Hal ini mencakup:

1. Penggunaan enkripsi *end-to-end*, *firewall* canggih, dan sistem deteksi intrusi yang didukung AI
2. Rutin melakukan *penetration testing* dan audit keamanan oleh pihak ketiga yang independen
3. Meningkatkan budaya keamanan melalui pelatihan dan simulasi serangan siber secara berkala
4. Menerapkan sistem deteksi *fraud* yang memadai untuk mendeteksi transaksi anomali secara real-time
5. Nasabah diimbau untuk tidak membagikan informasi rahasia seperti PIN, *password*, maupun OTP kepada siapa pun

Kedua, solusi kelembagaan dan regulasi. Regulator memiliki peran krusial dalam menciptakan ekosistem yang aman:

1. OJK harus lebih proaktif dalam melakukan pengawasan dan memberikan sanksi yang tegas
2. Regulator perlu menyusun standar teknis yang lebih detail dan wajib dipatuhi oleh bank
3. Diperlukan sinergi antara regulasi umum dan sektoral serta peningkatan kapasitas pengawasan dan literasi hukum

4. Bank Indonesia perlu mengevaluasi ulang sistem keamanan BI-Fast dan mempertimbangkan pembentukan lembaga independen untuk menilai keandalan sistem
5. Diperlukan harmonisasi regulasi antara UU PDP, UU Perbankan, dan regulasi sektoral OJK untuk menghindari tumpang tindih dan ketidakpastian hukum

Ketiga, komunikasi dan pemulihan kepercayaan. Komunikasi yang jelas dan transparan adalah kunci utama untuk memulihkan kepercayaan masyarakat pasca-insiden kebocoran data:

1. Bank harus segera mengumumkan kepada nasabah tentang insiden dengan informasi yang jujur dan jelas
2. Menunjukkan akuntabilitas melalui permintaan maaf secara terbuka dan penawaran bantuan nyata
3. Secara konsisten memberikan pembaruan mengenai proses perbaikan sistem keamanan
4. Bank DKI disarankan untuk melantai di Bursa Efek Indonesia (BEI) agar setiap kinerjanya dipantau dan diawasi oleh pemegang saham publik

KESIMPULAN

Pertama, kasus kebocoran data Bank DKI tahun 2025 membuktikan bahwa keamanan perbankan modern tidak lagi cukup hanya mengandalkan prinsip kerahasiaan bank yang tradisional. Ancaman siber yang canggih menunjukkan adanya kerentanan pada tiga aspek utama: teknis (kelemahan sistem pembayaran BI-Fast dan ketiadaan sistem deteksi *fraud* yang memadai), prosedural (*External Partner Agreement* yang tidak berjalan semestinya dan lemahnya pengawasan internal), dan sumber daya manusia (keterlibatan internal dengan akses tingkat tinggi serta kurangnya budaya keamanan). Insiden ini mengakibatkan 807 transaksi anomali dengan nilai Rp227,1 miliar dan penetapan enam tersangka oleh Polri, dengan otak utama masih dalam pengejaran.

Kedua, meskipun kerangka hukum di Indonesia—khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, POJK Nomor 11/POJK.03/2022, serta POJK Nomor 34 Tahun 2025—telah memberikan landasan yang kuat, terdapat kesenjangan signifikan antara regulasi dan implementasi di lapangan. Lemahnya pengawasan, kurangnya kepatuhan bank terhadap prinsip kehati-hatian, serta belum optimalnya koordinasi antar regulator (OJK dan Bank Indonesia) menjadi tantangan kritis. Kelemahan pada infrastruktur BI-Fast dan peran ganda Bank Indonesia sebagai operator sekaligus pengawas juga menjadi sorotan.

Ketiga, dampak terberat dari kasus ini adalah terkikisnya kepercayaan masyarakat, yang merupakan fondasi vital bagi sektor perbankan. Seperti yang dikatakan pakar keamanan digital Stéphane Nappo: "Butuh 20 tahun untuk membangun reputasi dan hanya 5 menit untuk menghancurkannya". Pemulihan kepercayaan hanya bisa dicapai melalui transparansi, akuntabilitas penuh dari pihak bank, penguatan sistem keamanan, peningkatan literasi hukum masyarakat, serta reformasi sistemik pada infrastruktur pembayaran nasional.

Kasus kebocoran data Bank DKI merupakan peringatan keras bagi seluruh ekosistem perbankan. Untuk mencegah terulangnya insiden serupa, diperlukan solusi yang komprehensif, mulai dari investasi pada teknologi keamanan siber yang mutakhir, perbaikan prosedur internal dan pengawasan, peningkatan budaya keamanan, reformasi sistem BI-Fast, hingga penegakan regulasi yang lebih tegas oleh regulator. Diperlukan sinergi antara regulasi umum dan sektoral serta peningkatan kapasitas pengawasan dan literasi hukum agar perlindungan terhadap data pribadi nasabah dapat berjalan efektif dan memberikan kepastian hukum.

DAFTAR PUSTAKA

Aminah, Siti. (2025). "Respon Bank Pasca Kebocoran Data: Studi Kasus di Asia Tenggara." *Jurnal Manajemen Perbankan* 10(1): 45–60.

Basel Committee on Banking Supervision. (2006). *Basel II: International Convergence of Capital Measurement and Capital Standards*. Basel: Bank for International Settlements.

Otoritas Jasa Keuangan. (2022). Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Jakarta: OJK.

Otoritas Jasa Keuangan. (2022). Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Jakarta: OJK.

Otoritas Jasa Keuangan. (2022). Peraturan OJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Jakarta: OJK.

Otoritas Jasa Keuangan. (2025). Peraturan OJK Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah. Jakarta: OJK.

Republik Indonesia. (1998). Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Jakarta: Sekretariat Negara.

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

Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta: Sekretariat Negara.

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

Santoso, Rudi. (2024). "Analisis Faktor-Faktor Penyebab Kebocoran Data di Sektor Perbankan." *Jurnal Keamanan Siber* 5(2): 120–135.

Antaranews.com. (2025, 26 November). "Cegah Kejahatan Siber, BRI Edukasi Nasabah Pentingnya Jaga Kerahasiaan Data Transaksi Perbankan." Diakses dari https://www.antaranews.com.

Bisnis.com. (2025, 21 Desember). "Sederet Fakta Soal Peretasan Rp200 Miliar Via BI Fast, Apa Langkah OJK?" Diakses dari https://finansial.bisnis.com.

Detik.com. (2025, 21 Desember). "Usai Kasus Peretasan BI Fast, OJK Periksa Ketahanan Siber Seluruh BPD." Diakses dari https://finance.detik.com.

Fortuneidn.com. (2025, 29 April). "OJK Beri Peringatan Keras ke Bank DKI Terkait Sistem IT Error." Diakses dari https://www.fortuneidn.com.

Hukumonline.com. (2025). "Menakar Batas Hak Privasi di Sektor Perbankan." Diakses dari https://www.hukumonline.com.

Infobanknews.com. (2025, 28 April). "Soal Gangguan Sistem Bank DKI, OJK Bilang Begini." Diakses dari https://infobanknews.com.

Kompas.com. (2025, 16 April). "Bank DKI Bocor Rp 100 Miliar, Dirut Sebut Ada Peretasan Internal." Diakses dari https://money.kompas.com.

Kompas.com. (2025, 10 April). "Bank DKI Sudah Laporkan Gangguan Sistem ke Bareskrim Polri." Diakses dari https://nasional.kompas.com.

Kompas.com. (2025, 9 April). "Pramono Gandeng Auditor Internasional Usut Kebocoran Sistem Bank DKI." Diakses dari https://megapolitan.kompas.com.

Tempo.co. (2025, 16 Oktober). "Indonesia's Bank DKI Faces Cyber Attack, Irregular Transactions Reach Over US$15mn." Diakses dari https://en.tempo.co.

Tempo.co. (2025, 4 November). "Police Arrest Six Suspects in Rp200 Billion Bank Jakarta System Breach." Diakses dari https://en.tempo.co.

Tempo.co. (2025, 25 November). "Payment System Security Flaws." Diakses dari https://en.tempo.co.