Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia

Ilman Maulana Kholis
UIN Sunan Kalijaga Yogyakarta
E-mail*: 23103040125@student.uin-suka.ac.id*

Abstract: *The rapid development of information technology has had a significant impact on the banking sector, while simultaneously increasing the risk of cyberattacks, particularly ransomware. This study aims to analyze the legal implications of the 2023 ransomware attack on Bank Syariah Indonesia (BSI), focusing on personal data protection and the effectiveness of existing regulations, namely the Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (ITE Law). Using a normative juridical approach and qualitative descriptive analysis, the study finds that although national regulations comprehensively cover personal data protection, their implementation in the BSI case faces several challenges, including delayed incident reporting and low institutional readiness against cyber threats. A comparison with the European Union's General Data Protection Regulation (GDPR) reveals gaps in regulatory oversight, institutional capacity, and cross-sector collaboration in Indonesia. This study recommends strengthening regulatory enforcement, improving data security literacy, establishing an independent supervisory body, and enhancing inter-agency cooperation to build a more resilient data protection ecosystem in the national banking sector.*
Keywords: *ransomware, personal data protection, cybersecurity, PDP Law, ITE Law, banking sector.*

Abstrak: Pesatnya perkembangan teknologi informasi telah membawa dampak signifikan terhadap sektor perbankan, sekaligus meningkatkan risiko serangan siber, khususnya ransomware. Penelitian ini bertujuan untuk menganalisis implikasi hukum dari kasus serangan ransomware terhadap Bank Syariah Indonesia (BSI) pada tahun 2023, dengan fokus pada perlindungan data pribadi dan efektivitas regulasi yang berlaku, yaitu UU Perlindungan Data Pribadi (UU PDP) dan UU Informasi dan Transaksi Elektronik (UU ITE). Menggunakan pendekatan yuridis-normatif dan analisis deskriptif kualitatif, penelitian ini menemukan bahwa meskipun regulasi nasional telah mengatur secara komprehensif mengenai perlindungan data pribadi, penerapannya dalam kasus BSI masih menemui berbagai hambatan, termasuk keterlambatan pelaporan insiden dan rendahnya kesiapan institusi perbankan terhadap ancaman siber. Perbandingan dengan standar GDPR Uni Eropa menunjukkan

bahwa Indonesia masih memiliki gap dalam pengawasan, kapasitas kelembagaan, dan kolaborasi lintas sektor. Penelitian ini merekomendasikan penguatan penegakan regulasi, peningkatan literasi keamanan data, pembentukan lembaga pengawas independen, serta peningkatan kerja sama antar lembaga untuk menciptakan ekosistem perlindungan data yang lebih tangguh di sektor perbankan nasional.
Kata Kunci: *ransomware, perlindungan data pribadi, keamanan siber, UU PDP, UU ITE, sektor perbankan.*

Pendahuluan

Pesatnya perkembangan teknologi informasi di era digital telah mengubah secara fundamental cara manusia berinteraksi, baik dalam konteks sosial maupun ekonomi. Teknologi informasi yang kini menjadi bagian integral dari kehidupan sehari-hari tidak hanya memberikan dampak positif dalam bentuk kemudahan akses dan efisiensi, tetapi juga menghadirkan tantangan baru berupa meningkatnya ancaman keamanan siber.[1] Fenomena ini menuntut perhatian khusus dari berbagai pihak, terutama dalam mengantisipasi dan menangani bentuk kejahatan baru yang berbasis digital atau dikenal sebagai kejahatan siber (cybercrime).[2] Menurut laporan resmi dari Surfshark, Indonesia tercatat sebagai negara urutan ke-14 di dunia dengan jumlah kasus kejahatan siber tertinggi.[3] Data ini mengindikasikan urgensi yang tinggi bagi negara untuk mengambil langkah-langkah preventif dan represif guna menangani ancaman siber yang terus meningkat.

Cybercrime mencakup berbagai aktivitas kriminal yang dilakukan dengan memanfaatkan teknologi komputer atau data digital.[4] Salah satu bentuk kejahatan siber yang paling signifikan adalah serangan

[1] F Muin, "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi," *IDRIS: InDonesian Journal of Islamic Studies* 1, no. 1 (2023): 97–113, http://yambus-lpksa.com/index.php/IDRIS/article/view/22.

[2] Duygu Solak and Murat Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Social and Behavioral Sciences* 182 (2015): 590–95, https://doi.org/10.1016/j.sbspro.2015.04.787.

[3] Surfshark, "Global Data Breach Statistics," 2025, https://surfshark.com/research/data-breach-monitoring?country=id.

[4] Doris Karina Oropeza Mendoza, "The Vulnerability of Cyberspace - The Cyber Crime," *Journal of Forensic Sciences & Criminal Investigation* 2, no. 1 (2017), https://doi.org/10.19080/jfsci.2017.02.555576.

terhadap sektor perbankan, yang sering kali menargetkan informasi pribadi individu yang bersifat sensitif.[5] Salah satu kasus yang menjadi sorotan adalah serangan ransomware yang menimpa Bank Syariah Indonesia (BSI) pada 14 Mei 2023. Dalam kasus ini, peretas berhasil mengakses 15 juta catatan pelanggan, informasi karyawan, dan sekitar 1,5 terabyte data internal dan membocorkan 8.133 file, termasuk data pribadi 24.437 pegawai, seperti nomor ponsel, alamat email, alamat rumah, nomor identifikasi karyawan, serta dokumen internal penting lainnya, hal ini disampaikan Aprianto dalam cuitan Twitter (sekarang X) yang dimuat dalam laman berita nasional.[6] Dampak dari insiden ini tidak terbatas pada operasional bank saja, tetapi juga mengancam privasi dan keamanan informasi pribadi karyawan dan mantan karyawan. Kasus ini memperlihatkan celah keamanan yang serius di sektor perbankan Indonesia, sekaligus menimbulkan pertanyaan mengenai kesiapan institusi keuangan dalam menghadapi ancaman siber yang terus berkembang.[7]

Penelitian terdahulu telah mengidentifikasi bahwa kejahatan siber, khususnya ransomware, terus mengalami peningkatan seiring dengan semakin meluasnya penggunaan teknologi digital dalam transaksi perbankan dan keuangan. Studi yang dilakukan oleh Kshetri (2024) menunjukkan bahwa ransomware menjadi salah satu bentuk kejahatan siber yang paling merugikan, dengan dampak finansial dan reputasi yang besar bagi perusahaan korban.[8] Temuan ini didukung oleh penelitian oleh Alwashali. (2021), yang menekankan bahwa

---

[5] Nida Rafa Arofah and Yeni Priatnasari, "Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional," *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19, https://doi.org/10.21831/jpai.v18i2.35872.

[6] Agus Ramadhan, "15 Juta Data Nasabah BSI Dicuri LockBit, Pakar Siber Minta Perbankan Lainnya Lakukan Mitigasi," Tribunnews, 2023, https://aceh.tribunnews.com/2023/05/13/15-juta-data-nasabah-bsi-dicuri-lockbit-pakar-siber-minta-perbankan-lainnya-lakukan-mitigasi?page=all#goog_rewarded.

[7] Irma Nurrizki Rahmawati et al., "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah," *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora* 3, no. 2 (2023): 208–15, http://pijarpemikiran.com/index.php/Aufklarung.

[8] Naresh Kshetri et al., "CryptoRAN: A Review on Cryptojacking and Ransomware Attacks W.R.T. Banking Industry - Threats, Challenges, & Problems," in *Proceedings - 2nd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2024*, 2024, 523–28, https://doi.org/10.1109/InCACCT61598.2024.10550970.

kerugian akibat serangan ransomware tidak hanya berupa kehilangan data, tetapi juga merusak kepercayaan publik terhadap institusi yang diserang.[9] Namun demikian, penelitian-penelitian sebelumnya cenderung berfokus pada dampak ekonomi secara umum, sementara analisis khusus terkait dampak hukum dan implikasi regulatif dari kasus ransomware di sektor perbankan Indonesia, khususnya dalam konteks perlindungan data pribadi, masih belum cukup mendalam. Kekurangan ini menunjukkan adanya gap penting yang perlu dijembatani melalui penelitian lanjutan yang secara khusus menelaah aspek hukum terkait pelanggaran data pribadi di sektor perbankan.

Secara normatif, Indonesia telah memiliki regulasi yang mengatur perlindungan data pribadi, khususnya melalui Undang-Undang Perlindungan Data Pribadi (UU PDP). Pasal 46 UU PDP secara tegas mengatur bahwa setiap pihak yang mengalami pelanggaran data wajib memberikan pemberitahuan tertulis kepada pihak yang terdampak dalam waktu maksimal 72 jam.[10] Dalam kasus serangan ransomware terhadap Bank Syariah Indonesia, kewajiban ini tampaknya tidak sepenuhnya terpenuhi,[11] menciptakan potensi pelanggaran tambahan dari sisi hukum yang memerlukan analisis mendalam. Di samping itu, hak perlindungan data pribadi juga dijamin dalam Konstitusi Indonesia sebagaimana tercantum dalam Pasal 28G ayat (1) UUD 1945, yang memberikan hak setiap individu atas perlindungan terhadap informasi pribadi dan rasa aman dari ancaman pelanggaran data.

Urgensi penelitian ini semakin kuat mengingat meningkatnya transaksi non-tunai yang secara masif diadopsi oleh masyarakat Indonesia, yang secara tidak langsung meningkatkan risiko terhadap

---

[9] Ali Ahmed Mohammed Ali Alwashali, Nor Azlina Abd Rahman, and Noris Ismail, "A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack," in *Proceedings - International Conference on Developments in ESystems Engineering, DeSE*, vol. 2021-December, 2021, 92–96, https://doi.org/10.1109/DESE54285.2021.9719456.

[10] Rosihan Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia," *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36, https://doi.org/10.36418/jurnalsostech.v2i5.336.

[11] Rendi Panca Wijanarko et al., "Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia," in *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, vol. 3, 2023, 106–15, https://doi.org/10.33005/sitasi.v3i1.436.

ancaman siber di sektor perbankan. Kasus BSI menjadi refleksi penting atas kebutuhan mendesak untuk mengevaluasi efektivitas regulasi dan mekanisme perlindungan data pribadi yang berlaku saat ini, serta bagaimana implementasinya secara praktis di lapangan.

Tujuan penelitian ini adalah untuk menganalisis secara kritis implikasi hukum dari kasus serangan ransomware terhadap Bank Syariah Indonesia pada tahun 2023, khususnya dalam konteks perlindungan data pribadi dan kepatuhan terhadap regulasi terkait. Penelitian ini bertujuan memberikan rekomendasi praktis maupun teoretis untuk memperkuat perlindungan data pribadi di sektor perbankan, sekaligus mendukung upaya pemerintah dan institusi terkait dalam meningkatkan keamanan siber di era digital.

Metodologi yang digunakan dalam penelitian ini adalah pendekatan normatif dengan metode penelitian hukum normatif (*normative legal research*). Pendekatan ini memanfaatkan analisis terhadap peraturan perundang-undangan yang relevan, termasuk UU Perlindungan Data Pribadi dan UU Informasi dan Transaksi Elektronik. Penelitian ini akan menggunakan berbagai bahan hukum sekunder seperti literatur hukum, jurnal ilmiah, putusan pengadilan, serta risalah hukum lainnya yang relevan. Data yang diperoleh akan dianalisis secara deskriptif kualitatif untuk mendapatkan gambaran yang komprehensif terkait permasalahan yang diangkat.

Berdasarkan latar belakang dan identifikasi celah penelitian yang telah dijelaskan, rumusan masalah dalam penelitian ini adalah: (1) Bagaimana implikasi hukum dari kasus serangan ransomware yang dialami oleh Bank Syariah Indonesia terhadap perlindungan data pribadi menurut regulasi yang berlaku di Indonesia? (2) Bagaimana efektivitas penerapan peraturan perlindungan data pribadi dalam kasus ini, dan langkah hukum apa yang perlu diambil oleh institusi perbankan untuk memitigasi risiko serupa di masa mendatang?

Hasil dan Pembahasan

Perkembangan Ancaman Siber di Indonesia dan Implikasinya terhadap Sektor Perbankan

Ancaman siber dalam beberapa tahun terakhir ini, khususnya serangan ransomware, telah mengalami eskalasi yang dramatis baik di tingkat global maupun nasional. Laporan Institute for Security and Technology mencatat bahwa sepanjang tahun 2023, serangan ransomware melonjak sebesar 73% dibandingkan tahun sebelumnya, dengan total 6.670 insiden yang dilaporkan.[12] Peningkatan ini menandakan bahwa kejahatan siber terus beradaptasi dengan perkembangan teknologi. Kelompok peretas seperti LockBit dan Clop semakin canggih dalam modus operandinya, mengadopsi teknik infiltrasi yang lebih terstruktur dan kompleks, serta secara khusus menargetkan sektor-sektor kritis seperti keuangan, layanan kesehatan, dan lembaga pemerintahan yang memiliki data bernilai tinggi.[13] Mereka memanfaatkan teknik eksploitasi kerentanan sistem yang belum diperbarui, rekayasa sosial (*social engineering*), serta pengembangan ransomware-as-a-service (RaaS) yang memungkinkan penyebaran malware secara masif.[14]

Tren serupa tercermin dari laporan Badan Siber dan Sandi Negara (BSSN), yang mencatat lebih dari 1,2 juta insiden serangan siber sepanjang tahun 2023. Dari jumlah tersebut, sektor perbankan menjadi salah satu target paling strategis, dengan 38 insiden ransomware yang dilaporkan secara resmi, menandakan adanya kerentanan signifikan

[12] Taylor Grossman and Trevaughn Smith, "2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge," IST, 2024, https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map.

[13] Nurul Monika Larasati and Rayyan Firdaus, "Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan," *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika* 2, no. 4 (2024): 102–9, https://doi.org/10.61132/merkurius.v2i4.151.

[14] Arlina Laras, "Begini Serangan Ransomware BSI Tahun Lalu, Mirip Dengan Penyebab PDN Down?," Bisnis.com, 2024, https://finansial.bisnis.com/read/20240627/90/1777564/begini-serangan-ransomware-bsi-tahun-lalu-mirip-dengan-penyebab-pdn-down?

dalam infrastruktur keamanan digital nasional.[15] Statistik lain dari Checkpoint Research menyebutkan bahwa sektor jasa keuangan di Indonesia menghadapi rata-rata 1.131 serangan siber setiap minggu sepanjang tahun 2022. Kondisi ini memperjelas bahwa sektor perbankan, sebagai tulang punggung transaksi ekonomi nasional, berada dalam tekanan besar untuk memperkuat ketahanan digitalnya.[16]

Kasus serangan ransomware terhadap Bank Syariah Indonesia (BSI) pada Mei 2023 menjadi ilustrasi nyata dari lemahnya pertahanan keamanan siber di sektor ini.[17] Dalam insiden tersebut, kelompok peretas LockBit berhasil menyusup ke sistem internal BSI melalui celah keamanan yang tercipta akibat pengaturan default pada perangkat yang belum dikonfigurasi ulang.[18] Melalui celah ini, LockBit mengenkripsi data internal bank dan berhasil memperoleh akses terhadap sekitar 1,5 terabyte data sensitif, termasuk data pribadi 15 juta nasabah dan informasi pegawai. Layanan perbankan BSI, termasuk ATM dan aplikasi perbankan digital, lumpuh selama beberapa hari, mengakibatkan gangguan besar pada transaksi keuangan masyarakat.[19]

Kronik awal kasus ini bermula pada 08 Mei 2023, pada tahap ini, gangguan tampak seperti masalah teknis biasa. Namun, kejanggalan mulai muncul karena akses ke layanan tidak kunjung pulih, dan transaksi nasabah terganggu dalam waktu yang lebih lama dari biasanya. Keterlambatan dalam pemulihan layanan menimbulkan keresahan di kalangan nasabah, terutama di wilayah Aceh yang sangat bergantung pada sistem perbankan syariah BSI untuk berbagai keperluan, termasuk pembayaran biaya ibadah haji. Ketidakpastian meningkat karena belum

[15] Indonesia Economic Outlook (IEO), "Kepincangan Digital: Ancaman Serius Di Balik Kesuksesan Sektor Keuangan Indonesia," IEO, 2024, https://ieofebui.com/ieorealizemoneter.

[16] PERBANAS Perhimpunan Bank Nasional, "Rawan Serangan Siber, Sektor Perbankan Perbesar Capex Untuk Investasi IT," PERBANAS, 2023.

[17] Defara Dhanya, "Daftar Serangan Ransomware Ke Lembaga Keuangan Indonesia: BI, BSI Dan Terbaru BRI," Tempo.co, 2024, https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490.

[18] Laras, "Begini Serangan Ransomware BSI Tahun Lalu, Mirip Dengan Penyebab PDN Down?"

[19] Galih Pratama, "Perbankan RI Sasaran Empuk Serangan Siber, Ini Faktanya," Infobanknews, 2023, https://infobanknews.com/perbankan-ri-sasaran-empuk-serangan-siber-ini-faktanya/#google_vignette.

adanya pernyataan resmi yang menjelaskan penyebab gangguan tersebut.[20]

Situasi semakin mengkhawatirkan ketika kelompok peretas LockBit 3.0, salah satu sindikat ransomware paling terkenal di dunia, mengklaim bertanggung jawab atas serangan tersebut. LockBit mengaku telah berhasil menyusup ke sistem internal BSI melalui kerentanan dalam konfigurasi perangkat yang masih menggunakan pengaturan default. Mereka mengklaim telah mengenkripsi sejumlah besar data dan berhasil mengambil alih sekitar 1,5 terabyte data sensitif, termasuk data pribadi milik kurang lebih 15 juta nasabah serta informasi karyawan.[21]

Ancaman LockBit tidak berhenti pada penyusupan data. Mereka memberikan ultimatum kepada BSI untuk membayar uang tebusan sebelum tenggat waktu 15 Mei 2023, dengan ancaman akan membocorkan data tersebut ke publik jika permintaan mereka tidak dipenuhi. Dalam periode krusial ini, BSI memilih untuk tidak memberikan respons langsung kepada publik terkait klaim tersebut. Pihak bank hanya mengumumkan bahwa mereka tengah berupaya memulihkan sistem dan memastikan keamanan data dan dana nasabah, tanpa mengonfirmasi ataupun menyangkal klaim LockBit secara eksplisit.[22]

Seiring berjalannya waktu dan melewati tenggat yang ditetapkan LockBit, dugaan kebocoran data mulai mencuat. Data-data yang diklaim dicuri diduga telah diunggah ke forum-forum di dark web, meskipun BSI bersikeras bahwa data nasabah tetap aman. Meski begitu, kepercayaan publik telah terlanjur terguncang. Laporan media

[20] Hesti Puji Lestari, "Kronologi BSI Diserang Ransomware Oleh Hacker Lockbit 3.0, Diduga Beraksi Sejak Libur Lebaran 2023," Bisnis.com, 2023, https://finansial.bisnis.com/read/20230514/90/1655733/kronologi-bsi-diserang-ransomware-oleh-hacker-lockbit-30-diduga-beraksi-sejak-libur-lebaran-2023.

[21] CNN, "Ransomware Lockbit 3.0 Klaim Lumpuhkan BSI Dan Curi Data Pengguna," CNN Indonesia, accessed May 20, 2025, https://www.cnnindonesia.com/teknologi/20230513093401-185-949046/ransomware-lockbit-30-klaim-lumpuhkan-bsi-dan-curi-data-pengguna.

[22] Agustinus Rangga Respati and Yoga Sukmana, "Perjalanan Kasus BSI, Dari Gangguan Layanan Sampai 'Hacker' Minta Tebusan," Kompas.com, 2023, https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all.

menunjukkan adanya penurunan drastis dalam tingkat kepercayaan dan loyalitas nasabah terhadap bank tersebut.[23]

Dalam upaya menangani serangan ini, BSI bekerja sama dengan berbagai otoritas nasional, termasuk Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia. Selain itu, penyelidikan lebih dalam dilakukan oleh Bareskrim Polri, terutama Direktorat Tindak Pidana Siber, untuk mengungkap mekanisme serangan dan pihak-pihak yang bertanggung jawab. Langkah-langkah mitigasi diintensifkan, termasuk memperbaiki kerentanan sistem dan meningkatkan protokol keamanan digital.[24]

Serangan ini mengungkap berbagai kelemahan struktural dalam sistem perlindungan data BSI, termasuk kurangnya pengawasan internal terhadap kerentanan perangkat, serta lemahnya penerapan kebijakan keamanan siber yang komprehensif. Di sisi regulatif, insiden ini menunjukkan perlunya implementasi lebih ketat terhadap ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mewajibkan setiap pengendali data pribadi untuk melaporkan insiden pelanggaran kepada subjek data secara transparan dalam waktu maksimal 72 jam. Kewajiban ini bertujuan untuk menjamin hak subjek data atas informasi terkait risiko yang mungkin timbul akibat kebocoran data mereka.

Dampak insiden ini tidak hanya bersifat teknis dan operasional, tetapi juga menyentuh aspek kepercayaan nasabah. Penelitian menunjukkan bahwa kepercayaan nasabah terhadap BSI menurun sebesar 47,6% pasca-serangan, sementara loyalitas nasabah turun drastis hingga 35,6%.[25] Angka-angka ini mencerminkan bahwa serangan siber bukan hanya mengancam kelangsungan operasional bank, tetapi juga berpotensi merusak reputasi jangka panjang dan stabilitas sektor keuangan nasional. Bank, yang berfungsi sebagai lembaga penyimpanan dan pengelolaan data pribadi dan finansial

[23] Lutfi Maulana and Nadia Fitriana, "Analisis Dampak Insiden BSI Eror Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang," *Rayah Al-Islam* 7, no. 3 (2023), https://doi.org/https://doi.org/10.37274/rais.v7i3.899.

[24] Lestari, "Kronologi BSI Diserang Ransomware Oleh Hacker Lockbit 3.0, Diduga Beraksi Sejak Libur Lebaran 2023."

[25] Maulana and Fitriana, "Analisis Dampak Insiden BSI Eror Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang."

masyarakat, dituntut untuk menjaga kepercayaan publik melalui sistem keamanan yang kokoh dan responsif.[26]

Dalam menghadapi peningkatan ancaman ini, sektor perbankan Indonesia perlu segera melakukan transformasi dalam kebijakan keamanan sibernya.[27] Investasi dalam teknologi keamanan terkini, seperti penggunaan sistem deteksi ancaman berbasis kecerdasan buatan (AI), peningkatan enkripsi data, dan penerapan kerangka kerja keamanan berbasis risiko (*risk-based security framework*) menjadi kebutuhan yang mendesak.[28] Pelatihan karyawan untuk meningkatkan kesadaran akan potensi serangan siber juga tidak dapat diabaikan, mengingat banyak serangan yang berhasil karena kelalaian manusia.

Lebih jauh, perlu dibangun ekosistem keamanan siber yang lebih kolaboratif antara lembaga perbankan, regulator seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia, serta Badan Siber dan Sandi Negara (BSSN). Kerja sama ini perlu difokuskan pada pertukaran informasi ancaman siber secara *real-time*, simulasi keamanan siber (*cybersecurity drills*), dan pengembangan standar keamanan minimum yang wajib diikuti seluruh institusi keuangan. Tanpa langkah-langkah strategis ini, sektor perbankan Indonesia akan tetap menjadi target empuk bagi pelaku kejahatan siber yang terus berkembang dalam kemampuan dan intensitas.[29]

Ancaman ransomware yang terus meningkat ini, seperti yang dialami oleh BSI, harus menjadi peringatan keras bahwa keamanan data dan infrastruktur digital bukan lagi pilihan, melainkan keniscayaan dalam mempertahankan ketahanan sistem keuangan nasional di era digital. Dengan kompleksitas dan kerusakan yang dapat diakibatkan

---

[26] Alva Yenica Nandavita, "Analisis Pengaruh Kepercayaan Nasabah Terhadap Risiko Menggunakan Layanan E-Banking," *AKSES: Jurnal Ekonomi Dan Bisnis* 17, no. 2 (2022), https://doi.org/10.31942/akses.v17i2.7463.

[27] Rochania Ayu Yunanda and Silvia Dewiyanti, "Digital Governance Strategies for Enhancing Sustainable Banking Ecosystem in Indonesia," in *2024 12th International Conference on Cyber and IT Service Management, CITSM 2024*, 2024, https://doi.org/10.1109/CITSM64103.2024.10775351.

[28] Agus Kurniati, "Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure," *Monas: Jurnal Inovasi Aparatur* 6, no. 2 (December 31, 2024): 154–65, https://doi.org/10.54849/monas.v6i2.251.

[29] Damar Apri Sudarmadi and Arthur Josias Simon Runturambi, "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 2, no. 2 (2019): 157–78, http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/28.

oleh serangan siber, hanya pendekatan yang komprehensif, proaktif, dan berbasis kolaborasi yang mampu memberikan perlindungan efektif terhadap data pribadi dan transaksi finansial masyarakat Indonesia.

Kerangka Hukum Perlindungan Data Pribadi di Indonesia

Kerangka hukum perlindungan data pribadi di Indonesia menjadi landasan penting dalam menjamin hak privasi warga negara. Secara normatif, perlindungan data pribadi di Indonesia baru mendapatkan pengaturan komprehensif dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini menjadi tonggak hukum yang memberikan legitimasi terhadap perlindungan hak atas data pribadi individu sebagai bagian dari hak asasi manusia yang tidak dapat dikurangi dalam keadaan apa pun.[30]

UU PDP mengklasifikasikan data pribadi ke dalam dua kategori, yakni data pribadi umum dan data pribadi spesifik. Klasifikasi ini penting mengingat data pribadi spesifik, seperti data kesehatan, data biometrik, data genetika, dan data finansial, memiliki risiko lebih besar terhadap individu jika disalahgunakan. Salah satu ketentuan penting dalam UU PDP adalah Pasal 46, yang mengatur kewajiban pelaporan insiden pelanggaran data pribadi. Pasal ini secara eksplisit menyatakan:

"Pengendali Data Pribadi wajib memberitahukan secara tertulis kepada Pemilik Data Pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam setelah diketahui terjadi kegagalan perlindungan Data Pribadi."

Kewajiban ini menandai pergeseran paradigma dari pendekatan reaktif menjadi proaktif, yang mana pelaku usaha atau institusi wajib memberikan transparansi kepada korban kebocoran data sebagai bagian dari prinsip akuntabilitas.[31]

---

[30] Nurmalasari Nurmalasari, "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum," *Syntax Idea* 3, no. 8 (2021): 1947–66, https://doi.org/10.46799/syntax-idea.v3i8.1414.

[31] Hijriani Hijriani et al., "Literasi Digital Perlindungan Hukum Terhadap Data Pribadi Nasabah Pengguna Electronic Wallet," *Sultra Research of Law* 5, no. 2 (2023): 85–95, https://doi.org/10.54297/surel.v5i2.59.

Lebih fundamental lagi, hak atas perlindungan data pribadi telah mendapat legitimasi konstitusional melalui Pasal 28G ayat (1) Undang-Undang Dasar 1945, yang menyatakan bahwa:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Pasal ini secara implisit menegaskan bahwa hak atas privasi, termasuk privasi data pribadi, merupakan bagian dari hak asasi manusia yang wajib dijaga oleh negara. Dalam konteks ini, data pribadi bukan hanya menjadi objek perlindungan hukum, melainkan inheren dengan identitas dan martabat individu.

Selain UU PDP, kerangka hukum perlindungan data juga didukung oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam UU Nomor 19 Tahun 2016. UU ITE mengatur sejumlah ketentuan terkait keamanan data, khususnya dalam Pasal 26 ayat (1) yang menyebutkan bahwa

"Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."

Ketentuan ini memberikan prinsip dasar perlindungan data dengan pendekatan berbasis consent, yang mensyaratkan persetujuan eksplisit dari pemilik data sebelum data tersebut diproses atau digunakan oleh pihak lain.

UU PDP memiliki kelebihan yaitu memberikan landasan hukum yang kuat dan lebih modern dibandingkan dengan ketentuan sebelumnya. Ia mengadopsi prinsip-prinsip yang selaras dengan General Data Protection Regulation (GDPR) Uni Eropa, seperti *lawfulness, fairness, transparency, purpose limitation,* dan *accountability.*[32] Kehadiran kewajiban pelaporan insiden juga meningkatkan transparansi dan memberikan hak kepada pemilik data untuk

[32] Paweł Drąg and Mateusz Szymura, "Technical and Legal Aspects of Database'S Security in the Light of Implementation of General Data Protection Regulation," *CBU International Conference Proceedings* 6 (2018): 1056–61, https://doi.org/10.12955/cbup.v6.1294.

mengetahui pelanggaran yang terjadi terhadap data mereka, sebuah mekanisme yang sebelumnya tidak tersedia secara eksplisit dalam UU ITE. Selain itu, dengan mempertegas sanksi administratif hingga pidana bagi pelanggaran data pribadi, UU PDP memperkuat posisi tawar individu terhadap korporasi dan institusi yang lalai.

Penegakan Hukum Terhadap Tindak Pidana Peretasan Bank Syariah Indonesia

Pesatnya kemajuan teknologi informasi tidak dapat dipungkiri telah membawa perubahan fundamental dalam lanskap sosial, ekonomi, dan hukum di era digital. Sementara teknologi memungkinkan efisiensi dalam transaksi keuangan dan komunikasi yang lebih cepat, ia juga membuka kerentanan baru dalam bentuk kejahatan siber. Salah satu fenomena paling nyata dari kerentanan ini adalah meningkatnya kasus ransomware yang menargetkan sektor perbankan,[33] sebagaimana tercermin dalam kasus serangan siber terhadap Bank Syariah Indonesia (BSI) pada Mei 2023.

Serangan ini tidak hanya mengguncang operasional bank, tetapi juga mengancam hak fundamental nasabah atas perlindungan data pribadinya. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi instrumen hukum utama yang dirancang untuk melindungi individu dari pelanggaran data pribadi. Dalam kerangka UU PDP, serangan ransomware yang menimpa BSI dapat dikualifikasikan sebagai bentuk kegagalan perlindungan data sebagaimana diatur dalam Pasal 46 UU PDP, yang mewajibkan setiap Pengendali Data Pribadi untuk melakukan pemberitahuan tertulis kepada subjek data paling lambat 72 jam setelah diketahui adanya insiden pelanggaran data.[34] Kewajiban ini merupakan manifestasi dari prinsip akuntabilitas dan transparansi, yang mewajibkan institusi keuangan seperti BSI untuk tidak hanya bertanggung jawab atas data yang mereka kelola, tetapi juga bersikap terbuka terhadap publik atas setiap pelanggaran yang terjadi.

Namun, dalam praktiknya, implementasi ketentuan ini

[33] Respati and Sukmana, "Perjalanan Kasus BSI, Dari Gangguan Layanan Sampai 'Hacker' Minta Tebusan."

[34] Nurul Monika Larasati and Rayyan Firdaus, "Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan."

menghadapi berbagai tantangan. Dalam kasus BSI, pemberitahuan kepada publik dan nasabah tidak dilakukan secara tepat waktu dan rinci sebagaimana dikehendaki UU PDP. Hal ini menunjukkan adanya kesenjangan serius antara norma regulatif dengan penerapan aktual di lapangan. Keterlambatan dan minimnya informasi yang disampaikan kepada publik tidak hanya memperburuk ketidakpercayaan nasabah, tetapi juga memperbesar risiko sekunder seperti pencurian identitas dan penipuan berbasis data pribadi. Ini mengindikasikan bahwa meskipun regulasi telah mengadopsi prinsip-prinsip perlindungan data modern, mekanisme pengawasan dan penegakan di Indonesia masih lemah.

Dilihat dari perspektif konstitusional, kegagalan dalam melindungi data pribadi juga dapat diinterpretasikan sebagai pelanggaran terhadap Pasal 28G ayat (1) UUD 1945 yang menjamin hak atas perlindungan diri pribadi dan rasa aman. Perlindungan terhadap data pribadi merupakan ekstensi dari hak privasi yang melekat pada setiap warga negara sebagai bagian dari hak asasi manusia. Dalam konteks ini, tidak hanya terjadi pelanggaran administratif, melainkan juga pelanggaran terhadap prinsip dasar negara hukum yang wajib melindungi hak-hak dasar warganya.[35]

Selain mekanisme administratif, implikasi hukum dari serangan ransomware ini juga harus dipertimbangkan dalam konteks pidana dan perdata. Secara pidana, Pasal 30 dan Pasal 46 UU ITE dapat diterapkan terhadap para pelaku yang melakukan akses ilegal terhadap sistem elektronik. Pasal 30 ayat (3) UU ITE secara tegas mengkriminalisasi akses tanpa izin yang menyebabkan kerugian, sedangkan Pasal 46 mengatur sanksi pidananya, yang dapat berupa hukuman penjara dan/atau denda. Dalam kasus BSI, tindakan kelompok LockBit yang menyusup ke sistem perbankan dan memperoleh data pribadi nasabah jelas memenuhi unsur-unsur tindak pidana tersebut.

Di sisi lain, potensi sanksi administratif terhadap BSI sebagai Pengendali Data Pribadi diatur dalam Pasal 57 dan Pasal 58 UU PDP, yang memungkinkan pemberian sanksi administratif berupa teguran, denda administratif, hingga pembatasan kegiatan pengolahan data. Kewajiban untuk segera memberitahukan kebocoran data kepada subjek data juga diperkuat oleh ketentuan dalam Peraturan OJK, PP

[35] Artanti Zahra Adisa and Andriyanto Adhi Nugroho, "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk," *Justisi* 10, no. 1 (2024): 242–56, https://doi.org/10.33506/js.v10i1.2980.

No. 71 Tahun 2019 tentang Sistem dan Transaksi Elektronik (PSTE), serta Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Dengan tidak optimalnya pemenuhan kewajiban tersebut, BSI berpotensi dikenai sanksi berlapis baik dari sisi perlindungan konsumen jasa keuangan maupun perlindungan data pribadi.

Dari sudut pandang hukum perdata, pelanggaran data pribadi yang terjadi membuka ruang gugatan ganti rugi berdasarkan Pasal 1365 KUH Perdata tentang perbuatan melawan hukum (onrechtmatige daad). Kerugian yang diderita nasabah, baik berupa kerugian materiil akibat penyalahgunaan data maupun kerugian immateriil berupa kehilangan rasa aman, dapat diklaim sebagai akibat langsung dari kelalaian bank dalam melindungi data pribadi.

Kerangka hukum nasional Indonesia telah menyediakan berbagai instrumen untuk menangani pelanggaran data pribadi akibat serangan ransomware, baik melalui jalur administratif, pidana, maupun perdata. Akan tetapi, efektivitas implementasinya masih dibayangi oleh lemahnya koordinasi antar lembaga pengawas, rendahnya kesadaran institusi dalam membangun sistem keamanan data yang memadai, serta kurangnya edukasi publik mengenai hak-hak mereka atas data pribadi. Ketiga faktor ini memperlihatkan bahwa perlindungan hukum yang ada, meskipun telah disusun dengan mengikuti perkembangan standar internasional, belum sepenuhnya efektif dalam memberikan rasa aman dan keadilan bagi korban pelanggaran data pribadi.

Evaluasi Efektivitas Penerapan Regulasi Perlindungan Data Pribadi dalam Praktik

Penerapan regulasi perlindungan data pribadi di Indonesia, khususnya melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), merupakan upaya normatif dalam merespons eskalasi ancaman kejahatan siber. Namun, efektivitas keduanya dalam mencegah dan menangani kebocoran data di sektor perbankan masih menjadi

perdebatan serius.[36] Secara normatif, kedua regulasi ini mengatur kewajiban perlindungan data, prinsip-prinsip keamanan siber, serta sanksi bagi pelanggaran. Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia menetapkan kewajiban yang ketat bagi pengendali data, termasuk institusi perbankan, untuk segera memberitahukan kepada pemilik data jika terjadi kebocoran data pribadi. UU PDP mengatur bahwa pemberitahuan tersebut harus dilakukan dalam waktu maksimal 72 jam setelah terjadinya insiden kebocoran, dengan tujuan memperkuat transparansi, akuntabilitas, serta memberikan kesempatan kepada pemilik data untuk mengambil langkah mitigasi terhadap risiko penyalahgunaan data mereka.[37]

Mekanisme ini sejalan dengan praktik terbaik internasional, seperti yang diterapkan dalam General Data Protection Regulation (GDPR) Uni Eropa, yang mengharuskan pemberitahuan serupa dalam waktu 72 jam. Di Indonesia, ketentuan ini diharapkan dapat meningkatkan kepercayaan publik terhadap perlindungan data oleh lembaga keuangan, mengingat sektor ini mengelola informasi yang sangat sensitif.[38]

Namun dalam praktiknya, banyak lembaga perbankan masih menghadapi tantangan untuk memenuhi ketentuan tersebut secara efektif. Hambatan utama meliputi kurangnya kesiapan infrastruktur deteksi insiden keamanan secara real-time, terbatasnya kapasitas tim keamanan siber untuk melakukan investigasi cepat, dan kekhawatiran terhadap reputasi institusi yang menyebabkan keterlambatan dalam pelaporan. Selain itu, beberapa institusi masih belum memiliki prosedur standar operasi (SOP) yang matang untuk tanggap darurat insiden kebocoran data, yang menyebabkan inkonsistensi dalam pelaksanaan

[36] Muh. Akbar Fhad Syahril and Ardiyanti Aris, "Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act," *Journal of Law Justice (JLJ)* 2, no. 3 (November 18, 2024): 198–205, https://doi.org/10.33506/jlj.v2i3.3711.

[37] Zulkham Sadat Zuwanda et al., "Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and Its Impact on the Fintech Industry in Indonesia," *West Science Law and Human Rights* 2, no. 04 (October 25, 2024): 421–28, https://doi.org/10.58812/wslhr.v2i04.1367.

[38] Andrian Andrian, "Bank Responsibility on Customer's Data Fraud in Indonesia," *International Journal of Social Science and Human Research* 06, no. 05 (May 25, 2023), https://doi.org/10.47191/ijsshr/v6-i5-63.

pelaporan kepada regulator maupun kepada pemilik data.[39]

Kondisi ini menunjukkan bahwa meskipun UU PDP sudah menyediakan kerangka hukum yang memadai, efektivitasnya sangat bergantung pada kesiapan internal lembaga perbankan dalam membangun sistem respons insiden yang cepat dan prosedural. Oleh karena itu, investasi lebih lanjut dalam teknologi deteksi ancaman, pelatihan keamanan siber, serta budaya transparansi di lingkungan institusi keuangan sangat dibutuhkan untuk memastikan kepatuhan yang lebih baik terhadap ketentuan UU PDP.

Studi kasus peretasan Bank Syariah Indonesia (BSI) tahun 2023 memperlihatkan bahwa meskipun regulasi sudah ada, tingkat kesiapan institusi masih jauh dari memadai. Investigasi menunjukkan lemahnya prosedur respons insiden serta rendahnya literasi keamanan siber di kalangan karyawan, yang membuka celah bagi serangan ransomware. Analisis lebih lanjut juga menunjukkan bahwa ketergantungan pada sistem yang belum mengikuti standar keamanan informasi internasional seperti ISO 27001 memperburuk risiko kebocoran data. Hambatan lain adalah minimnya audit keamanan berkala dan keterbatasan dalam infrastruktur teknologi, termasuk penggunaan konfigurasi default yang memperbesar potensi eksploitasi oleh pelaku kejahatan siber.[40]

Sebagai perbandingan, General Data Protection Regulation (GDPR) Uni Eropa menawarkan standar perlindungan data yang lebih ketat dengan sanksi yang lebih berat, yakni denda hingga 20 juta euro atau 4% dari total pendapatan tahunan global perusahaan, mana yang lebih besar. GDPR juga mewajibkan penunjukan Data Protection Officer (DPO) di setiap organisasi besar, suatu mekanisme yang terbukti efektif dalam mengawasi kepatuhan internal terhadap prinsip-prinsip perlindungan data. Negara-negara seperti Jerman dan Belanda telah menunjukkan bahwa penerapan GDPR secara ketat berkontribusi signifikan dalam menekan angka kebocoran data, bahkan mendorong peningkatan signifikan dalam tingkat kepercayaan publik terhadap

[39] Fachrul Razi, Hadi Tuasikal, and Dwi Pratiwi Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia," *Jurnal Indonesia Sosial Teknologi* 5, no. 12 (December 30, 2024): 6015–21, https://doi.org/10.59141/jist.v5i12.1285.

[40] Yusep Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *Jurnal Dinamika Global* Vol.7 No. 2 (2022): 295–316.

institusi keuangan.

Upaya pemerintah Indonesia melalui Badan Siber dan Sandi Negara (BSSN) sudah diarahkan pada penguatan lima pilar keamanan siber yang merujuk pada Global Cybersecurity Index (GCI), yakni aspek hukum, teknis, organisasi, kapasitas, dan kolaborasi. Namun, laporan GCI terbaru menunjukkan Indonesia masih berada di peringkat 77 dari 193 negara, menandakan adanya gap signifikan dalam kapasitas nasional, khususnya dalam regulasi dan implementasi kebijakan.[41] Rendahnya jumlah Computer Security Incident Response Teams (CSIRTs) di Indonesia menjadi salah satu kendala besar dalam menanggulangi insiden siber secara cepat dan efektif. CSIRTs berperan sebagai unit yang bertugas merespons, mengelola, dan memitigasi insiden siber, serta berfungsi sebagai pusat koordinasi antara sektor publik dan privat dalam menghadapi serangan digital. Sayangnya, jumlah CSIRT di Indonesia masih belum sebanding dengan kebutuhan, terutama di sektor-sektor vital seperti perbankan dan keuangan. Minimnya unit ini membuat deteksi dini, penanganan cepat, serta koordinasi respons terhadap kebocoran data dan serangan siber menjadi terhambat, yang pada akhirnya memperlemah implementasi efektif UU PDP dan UU ITE.[42]

Di sisi lain, inisiatif riset dan pengembangan (R&D) dalam bidang keamanan siber juga masih tergolong rendah. Padahal, dalam ekosistem keamanan siber global, R&D berperan penting untuk mengembangkan teknologi deteksi ancaman terbaru, membangun algoritme proteksi data yang lebih canggih, serta menghasilkan inovasi dalam teknik mitigasi insiden. Kurangnya investasi di bidang ini menyebabkan Indonesia sangat bergantung pada solusi keamanan siber dari luar negeri, yang belum tentu sepenuhnya kompatibel dengan kebutuhan dan kondisi lokal. Hal ini menjadi ironi, mengingat implementasi efektif UU PDP dan UU ITE memerlukan adaptasi

[41] Irnasya Shafira, "Menganalisis Strategi Keamanan Siber Nasional Indonesia," Center for Digital Society, 2021, https://cfds.fisipol.ugm.ac.id/id/2021/07/28/menganalisis-strategi-keamanan-siber-nasional-indonesia/.

[42] Razi, Tuasikal, and Pratiwi Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia."

teknologi yang mampu menjawab tantangan spesifik di Indonesia.[43]

Lebih jauh lagi, literasi publik terkait keamanan siber masih menjadi masalah mendasar. Banyak pengguna internet di Indonesia yang belum memahami pentingnya perlindungan data pribadi, konsekuensi dari penyebaran informasi sensitif, serta langkah-langkah pencegahan dasar terhadap serangan siber seperti phishing. Tanpa literasi publik yang memadai, ketentuan-ketentuan dalam UU PDP dan UU ITE sulit untuk diimplementasikan secara optimal karena pengguna sendiri tidak memiliki kesadaran yang cukup untuk melindungi data mereka atau memahami hak-hak mereka sebagai pemilik data. Kondisi ini memperbesar risiko terjadinya pelanggaran data dan menurunkan efektivitas upaya regulator dalam menegakkan aturan.[44]

Lebih jauh, Otoritas Jasa Keuangan (OJK) telah menerbitkan POJK Nomor 11/POJK.03/2022 tentang Pemanfaatan Teknologi Informasi oleh Bank Umum, yang mengatur proses identifikasi aset, deteksi insiden, serta pemulihan layanan. Melalui Surat Edaran OJK yang lebih rinci, bank diwajibkan melakukan inventarisasi aset TI, menjaga dokumentasi sistemik, serta memiliki rencana tanggap darurat terhadap insiden siber. Namun dalam implementasi, masih banyak bank yang belum melakukan uji ketahanan siber secara reguler, belum lagi faktor keterbatasan sumber daya manusia yang kompeten di bidang keamanan siber. Hal ini menunjukkan bahwa regulasi saja tidak cukup tanpa adanya komitmen kuat dari manajemen puncak dan investasi berkelanjutan dalam teknologi keamanan.

Kolaborasi lintas sektor juga menjadi elemen vital. Kerja sama antara sektor perbankan, regulator, dan komunitas siber belum berjalan optimal, berbeda dengan praktik di negara maju yang telah mengembangkan platform berbagi informasi ancaman (threat intelligence sharing) secara real-time. Di Indonesia, inisiatif semacam

---

[43] Oky Syalendro, Arief Fahmi Lubis, and R Yusak Andri Ende Putra, "Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases," *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 4, no. 1 (December 30, 2024): 335–47, https://doi.org/10.57235/aurelia.v4i1.3708.

[44] Aulia Alayna Suvil et al., "Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020," *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL* 3, no. 4 (August 28, 2024): 70–80, https://doi.org/10.55606/jhpis.v3i4.4235.

ini masih sporadis dan kurang terintegrasi. Akibatnya, respons terhadap serangan siber bersifat reaktif ketimbang preventif.[45]

Mengatasi tantangan ini membutuhkan pendekatan multi-dimensi. Pelatihan keamanan siber harus menjadi agenda wajib, tidak hanya untuk tim TI tetapi juga seluruh karyawan perbankan, karena manusia tetap menjadi titik lemah utama dalam pertahanan siber. Di samping itu, diperlukan pembentukan lembaga pengawas independen sebagaimana diamanatkan oleh UU PDP untuk menjamin penerapan standar perlindungan data yang seragam dan terukur. Penerbitan undang-undang khusus tentang kejahatan siber, sebagaimana direkomendasikan para ahli, juga menjadi urgensi mengingat kompleksitas ancaman siber yang terus berkembang melampaui batas yurisdiksi tradisional.

Dengan memperkuat kerangka regulasi, meningkatkan kapasitas institusi, serta mengedukasi publik tentang pentingnya literasi keamanan digital, Indonesia dapat bergerak menuju ekosistem keuangan digital yang lebih aman, tangguh, dan terpercaya di tengah dinamika ancaman siber global yang kian kompleks

Kesimpulan

Berdasarkan analisis yang telah dilakukan, penelitian ini menemukan bahwa serangan ransomware terhadap Bank Syariah Indonesia (BSI) pada tahun 2023 memberikan gambaran konkret mengenai implikasi hukum kebocoran data pribadi di sektor perbankan Indonesia. Dalam konteks regulasi nasional, UU Perlindungan Data Pribadi (UU PDP) dan UU Informasi dan Transaksi Elektronik (UU ITE) telah menyediakan landasan hukum untuk perlindungan data pribadi dan penanganan insiden kebocoran data. Secara normatif, UU PDP melalui Pasal 46 mewajibkan pengendali data untuk memberitahukan pelanggaran dalam waktu maksimal 72 jam, sementara UU ITE memberikan ketentuan pidana atas akses ilegal terhadap sistem elektronik.

Namun, efektivitas penerapan regulasi tersebut dalam kasus BSI memperlihatkan sejumlah kelemahan. Di antaranya adalah

[45] Diny Luthfah, "Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia," *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 2023, 259–67, https://doi.org/10.25105/pdk.v9i1.18643.

keterlambatan dalam pemberitahuan kepada subjek data, minimnya kesiapan teknis institusi dalam menghadapi serangan siber, dan rendahnya literasi keamanan data di tingkat operasional. Hambatan implementasi ini diperparah oleh keterbatasan kapasitas sumber daya manusia, minimnya audit keamanan berkala, serta absennya lembaga pengawas independen yang mengawasi kepatuhan institusi terhadap ketentuan perlindungan data pribadi.

Penelitian ini juga menunjukkan bahwa, dibandingkan dengan best practices internasional seperti General Data Protection Regulation (GDPR) Uni Eropa, regulasi di Indonesia masih membutuhkan penguatan, baik dalam aspek normatif maupun implementatif. Ketiadaan mekanisme pengawasan yang efektif, ketidaksiapan dalam prosedur respons insiden, dan kurangnya kolaborasi lintas sektor menjadi faktor yang memperlemah sistem pertahanan data pribadi di sektor perbankan.

Adapun keterbatasan penelitian ini terletak pada ruang lingkup analisis yang lebih difokuskan pada studi kasus BSI dan regulasi nasional, tanpa melakukan pendekatan empiris melalui survei atau wawancara mendalam dengan pemangku kepentingan terkait seperti regulator, pelaku industri perbankan, maupun komunitas keamanan siber. Selain itu, penelitian ini belum sepenuhnya mengkaji secara komparatif model perlindungan data di negara-negara Asia Tenggara yang memiliki karakteristik pasar digital yang serupa dengan Indonesia.

Referensi

(IEO), Indonesia Economic Outlook. "Kepincangan Digital: Ancaman Serius Di Balik Kesuksesan Sektor Keuangan Indonesia." IEO, 2024. https://ieofebui.com/ieorealizemoneter.

Agus Kurniati. "Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure." *Monas: Jurnal Inovasi Aparatur* 6, no. 2 (December 31, 2024): 154–65. https://doi.org/10.54849/monas.v6i2.251.

Ali Alwashali, Ali Ahmed Mohammed, Nor Azlina Abd Rahman, and Noris Ismail. "A Survey of Ransomware as a Service (RaaS) and

Methods to Mitigate the Attack." In *Proceedings - International Conference on Developments in ESystems Engineering, DeSE*, 2021-December:92–96, 2021. https://doi.org/10.1109/DESE54285.2021.9719456.

Andrian, Andrian. "Bank Responsibility on Customer's Data Fraud in Indonesia." *International Journal of Social Science and Human Research* 06, no. 05 (May 25, 2023). https://doi.org/10.47191/ijsshr/v6-i5-63.

Arofah, Nida Rafa, and Yeni Priatnasari. "Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional." *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19. https://doi.org/10.21831/jpai.v18i2.35872.

Artanti Zahra Adisa, and Andriyanto Adhi Nugroho. "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk." *Justisi* 10, no. 1 (2024): 242–56. https://doi.org/10.33506/js.v10i1.2980.

Aulia Alayna Suvil, Firdaus Firdaus, M. Arif Ramadhan, Wanda Darma Putra, and Dwi Putri Lestarika. "Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020." *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL* 3, no. 4 (August 28, 2024): 70–80. https://doi.org/10.55606/jhpis.v3i4.4235.

CNN. "Ransomware Lockbit 3.0 Klaim Lumpuhkan BSI Dan Curi Data Pengguna." CNN Indonesia. Accessed May 20, 2025. https://www.cnnindonesia.com/teknologi/20230513093401-185-949046/ransomware-lockbit-30-klaim-lumpuhkan-bsi-dan-curi-data-pengguna.

Dhanya, Defara. "Daftar Serangan Ransomware Ke Lembaga Keuangan Indonesia: BI, BSI Dan Terbaru BRI." Tempo.co, 2024. https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490.

Drąg, Paweł, and Mateusz Szymura. "Technical and Legal Aspects of Database'S Security in the Light of Implementation of General Data Protection Regulation." *CBU International Conference Proceedings* 6 (2018): 1056–61.

https://doi.org/10.12955/cbup.v6.1294.

Grossman, Taylor, and Trevaughn Smith. "2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge." IST, 2024. https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map.

Hijriani, Hijriani, Muh. Nadzirin Anshari Nur, Adnan Ali, Azis Ali, and Winner A. Siregar. "Literasi Digital Perlindungan Hukum Terhadap Data Pribadi Nasabah Pengguna Electronic Wallet." *Sultra Research of Law* 5, no. 2 (2023): 85–95. https://doi.org/10.54297/surel.v5i2.59.

Kshetri, Naresh, Mir Mehedi Rahman, Sayed Abu Sayeed, and Irin Sultana. "CryptoRAN: A Review on Cryptojacking and Ransomware Attacks W.R.T. Banking Industry - Threats, Challenges, & Problems." In *Proceedings - 2nd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2024*, 523–28, 2024. https://doi.org/10.1109/InCACCT61598.2024.10550970.

Laras, Arlina. "Begini Serangan Ransomware BSI Tahun Lalu, Mirip Dengan Penyebab PDN Down?" Bisnis.com, 2024. https://finansial.bisnis.com/read/20240627/90/1777564/begini-serangan-ransomware-bsi-tahun-lalu-mirip-dengan-penyebab-pdn-down?

Lestari, Hesti Puji. "Kronologi BSI Diserang Ransomware Oleh Hacker Lockbit 3.0, Diduga Beraksi Sejak Libur Lebaran 2023." Bisnis.com, 2023. https://finansial.bisnis.com/read/20230514/90/1655733/kronologi-bsi-diserang-ransomware-oleh-hacker-lockbit-30-diduga-beraksi-sejak-libur-lebaran-2023.

Luthfah, Diny. "Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia." *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 2023, 259–67. https://doi.org/10.25105/pdk.v9i1.18643.

Luthfi, Rosihan. "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia." *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36.

https://doi.org/10.36418/jurnalsostech.v2i5.336.

Maulana, Lutfi, and Nadia Fitriana. "Analisis Dampak Insiden BSI Eror Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang." *Rayah Al-Islam* 7, no. 3 (2023). https://doi.org/https://doi.org/10.37274/rais.v7i3.899.

Muin, F. "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi." *IDRIS: InDonesian Journal of Islamic Studies* 1, no. 1 (2023): 97–113. http://yambus-lpksa.com/index.php/IDRIS/article/view/22.

Nandavita, Alva Yenica. "Analisis Pengaruh Kepercayaan Nasabah Terhadap Risiko Menggunakan Layanan E-Banking." *AKSES: Jurnal Ekonomi Dan Bisnis* 17, no. 2 (2022). https://doi.org/10.31942/akses.v17i2.7463.

Nurmalasari, Nurmalasari. "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum." *Syntax Idea* 3, no. 8 (2021): 1947–66. https://doi.org/10.46799/syntax-idea.v3i8.1414.

Nurul Monika Larasati, and Rayyan Firdaus. "Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan." *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika* 2, no. 4 (2024): 102–9. https://doi.org/10.61132/merkurius.v2i4.151.

Oropeza Mendoza, Doris Karina. "The Vulnerability of Cyberspace - The Cyber Crime." *Journal of Forensic Sciences & Criminal Investigation* 2, no. 1 (2017). https://doi.org/10.19080/jfsci.2017.02.555576.

Perhimpunan Bank Nasional, PERBANAS. "Rawan Serangan Siber, Sektor Perbankan Perbesar Capex Untuk Investasi IT." PERBANAS, 2023.

Pratama, Galih. "Perbankan RI Sasaran Empuk Serangan Siber, Ini Faktanya." Infobanknews, 2023. https://infobanknews.com/perbankan-ri-sasaran-empuk-serangan-siber-ini-faktanya/#google_vignette.

Rahmawati, Irma Nurrizki, Nova Rahmadani, Diyah Rosita Heni, and Sandro Kevin. "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah." *Aufklarung: Jurnal Pendidikan,*

Sosial Dan Humaniora 3, no. 2 (2023): 208–15. http://pijarpemikiran.com/index.php/Aufklarung.

Ramadhan, Agus. "15 Juta Data Nasabah BSI Dicuri LockBit, Pakar Siber Minta Perbankan Lainnya Lakukan Mitigasi." Tribunnews, 2023. https://aceh.tribunnews.com/2023/05/13/15-juta-data-nasabah-bsi-dicuri-lockbit-pakar-siber-minta-perbankan-lainnya-lakukan-mitigasi?page=all#goog_rewarded.

Razi, Fachrul, Hadi Tuasikal, and Dwi Pratiwi Markus. "Implementation and Challenges of the Personal Data Protection Law in Indonesia." *Jurnal Indonesia Sosial Teknologi* 5, no. 12 (December 30, 2024): 6015–21. https://doi.org/10.59141/jist.v5i12.1285.

Respati, Agustinus Rangga, and Yoga Sukmana. "Perjalanan Kasus BSI, Dari Gangguan Layanan Sampai 'Hacker' Minta Tebusan." Kompas.com, 2023. https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all.

Shafira, Irnasya. "Menganalisis Strategi Keamanan Siber Nasional Indonesia." Center for Digital Society, 2021. https://cfds.fisipol.ugm.ac.id/id/2021/07/28/menganalisis-strategi-keamanan-siber-nasional-indonesia/.

Solak, Duygu, and Murat Topaloglu. "The Perception Analysis of Cyber Crimes in View of Computer Science Students." *Procedia - Social and Behavioral Sciences* 182 (2015): 590–95. https://doi.org/10.1016/j.sbspro.2015.04.787.

Sudarmadi, Damar Apri, and Arthur Josias Simon Runturambi. "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 2, no. 2 (2019): 157–78. http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/28.

Surfshark. "Global Data Breach Statistics," 2025. https://surfshark.com/research/data-breach-monitoring?country=id.

Syahril, Muh. Akbar Fhad, and Ardiyanti Aris. "Strategies and

Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act." *Journal of Law Justice (JLJ)* 2, no. 3 (November 18, 2024): 198–205. https://doi.org/10.33506/jlj.v2i3.3711.

Syalendro, Oky, Arief Fahmi Lubis, and R Yusak Andri Ende Putra. "Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases." *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 4, no. 1 (December 30, 2024): 335–47. https://doi.org/10.57235/aurelia.v4i1.3708.

Wijanarko, Rendi Panca, Moch Rezeki Setiawan, Siti Mukaromah, and Abdul Rezha Efrat Najaf. "Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia." In *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 3:106–15, 2023. https://doi.org/10.33005/sitasi.v3i1.436.

Yunanda, Rochania Ayu, and Silvia Dewiyanti. "Digital Governance Strategies for Enhancing Sustainable Banking Ecosystem in Indonesia." In *2024 12th International Conference on Cyber and IT Service Management, CITSM 2024*, 2024. https://doi.org/10.1109/CITSM64103.2024.10775351.

Yusep Ginanjar. "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara." *Jurnal Dinamika Global* Vol.7 No. 2 (2022): 295–316.

Zuwanda, Zulkham Sadat, Loso Judijanto, Hendri Khuan, and Andri Triyantoro. "Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and Its Impact on the Fintech Industry in Indonesia." *West Science Law and Human Rights* 2, no. 04 (October 25, 2024): 421–28. https://doi.org/10.58812/wslhr.v2i04.1367.