Konsensus : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi
Volume. 3 Nomor. 1 Februari 2026
E-ISSN : 3048-1325; P-ISSN : 3048-4405, Hal 29-36
DOI: https://doi.org/10.62383/konsensus.v3i1.1517
Tersedia: https://journal.appisi.or.id/index.php/konsensus

Urgensi Pembentukan Undang Undang Keamanan Keuangan Siber: Melindungi Sistem Finansial di Sektor Digital

Sabila Helmalia Putri
Program Studi Ilmu Hukum, Universitas Pendidikan Ganesha, Indonesia

Penulis Korespondensi: sabila@student.undiksha.ac.id

Abstract. *Rapid developments related to technology are spreading rapidly in human life. The rapid development of this technology definitely brings positive and negative currents in its application. The higher the development, the greater the opportunity for negative impacts for irresponsible people. The utilization of technological developments in the financial sector is considered to greatly facilitate a person in carrying out economic activities. Armed with just one application, someone can make banking transfers, investments and their utilization in other economic activities. However, along with the ease and effectiveness of digital finance, there are also digital crimes that can harm many people in the banking world such as physing, malware, ransomware and so on. This type of research is a normative juridical research that focuses on laws and regulations to provide legal reformulation related to digital financial security finance to strengthen the defense of financial system protection in the digital sector which is very much needed in this increasingly sophisticated modern era.*

Keywords: *Technology, security, digital finance, economy, urgency of legal formation.*

Abstrak. Perkembangan pesat terkait dengan teknologi merebak pesat di dalam kehidupan manusia. Pesatnya perkembangan teknologi ini pasti membawa arus positif dan negatif dalam pengaplikasiannya. Semakin tinggi perkembangan tersebut maka akan semakin besar pula membuka peluang berupa dampak negatif bagi oknum-oknum yang tidak bertanggung jawab. Pemanfaatan perkembangan teknologi dalam sektor keuangan dirasa sangat memudahkan seseorang dalam melakukan kegiatan ekonomi. Hanya dengan berbekal satu aplikasi maka seseorang dapat melakukan transfer perbankan, investasi maupun pemanfaatannya dalam kegiatan ekonomi lainnya. Akan tetapi seiring dengan dimanjakannya dalam kemudahan dan keefektivan keuangan digital, maka terdapat pula kejahatan-kejahatan digital yang mampu merugikan banyak orang di dunia perbankan seperti *physing, malware, ransomware* dan lain sebagainya. Jenis penelitian ini merupakan penelitian yuridis normatif yang berfokus pada peraturan perundang undangan untuk memberikan reformulasi hukum terkait dengan keamanan keuangan digital untuk mengkokohkan pertahanan perlindungan sistem finansial di sektor digital sangat dibutuhkan di era moderen yang semakin canggih ini.

Kata kunci: Teknologi, keamanan, keuangan digital, ekonomi, urgensi pembentukan hukum.

1. LATAR BELAKANG

Dewasa ini perkembangan digital telah mendominasi lebih dari setengah sektor kehidupan. Perkembangan teknologi yang semakin hari semakin pesat telah membantu hampir dari seluruh aktivitas manusia seperti berkomunikasi, bekerja, berniaga bahkan sampai pengelolaan keuanganpun saat ini dikelola dengan sistem digital. Modernisasi kehidupan manusia dalam sektor keuangan ditandai dengan peluncuran aplikasi keuangan digital, dengan peluncuran ini memberikan akses bagi seluruh manusia untuk dapat melakukan transaksi secara digital yang cepat, tepat dan efisien. Dengan pemanfaatan perangkat *mobile banking* ini maka seseorang tak hanya dapat melakukan kegiatan transaksi perbankan akan tetapi aplikasi ini juga dapat menjadi media atau sarana investasi seseorang tanpa harus mengunjungi kantor atau pihak terkait untuk dapat melakukan kegiatan ini. Selain itu membayar tagihan, membeli keperluan seperti pulsa dan lainnya, mengirim uang serta pembayaran melalui barcode juga dapat

Artikel Masuk: 26 November 2025; Revisi: 30 Desember 2025; Diterima: 30 Januari 2025;
Terbit: 03 Februari 2026

dilakukan oleh aplikasi *mobilebanking.*

Meskipun telah sangat dimanjakan dengan berbagai manfaat dari aplikasi keuangan digital tersebut, perlu digarisbawahi juga bahwasanya perkembangan teknologi yang semakin pesat juga akan menghadirkan dampak-dampak negatif yang dibawanya. Hal ini tentu menjadi ketakutan baru bagi semua orang yang menggunaan aplikasi ini. Semakin cepat teknologi dapat diakses, semakin banyak perubahan dan perkembangan yang terjadi maka semakin tinggi pula risiko yang dihasilkan. Beberapa ancaman yang dapat terjadi dalam penggunaan aplikasi ini seperti serangan siber atau *cybercrime*, pencurian identitas pengguna, peretasan akun pengguna, pencurian saldo menjadi isu yang tidak bisa diabaikan (Azizah et al., 2024).

Seiring dengan pesatnya pengguna aplikasi keuangan berbasis digital ini maka diperlukan adanya suatu regulasi hukum yang mampu menjadi payung hukum untuk melindungi sistem finansial di sektor digital Indonesia. Jika tidak dilakukan tindakan preventif dan perbaikan dalam permasalah tersebut, maka korban yang dirugikan akan semakin bertambah. Hal ini sama saja dengan membuka kesempatan baru bagi para penjahat digital untuk melebarkan sayap dan melancarkan aksinya. Salah satu kejahatan siber yang pernah terjadi di tahun 2023 tepatnya pada tanggal 8 Mei yang merupakan serangan *ransomware* menimpa Bank Syariah Indonesia (BSI). Serangan ini berakibat fatal bagi BSI pasalnya akibat serangan ini BSI mengalami gangguan layanan yang melumpuhkan operasional perbankan dan dicurinya data pribadi sebanyak 15 juta nasabah dan pegawai (Putri & Yusuf, 2025).

Kejahatan digital atau cybercrime ini perlu selalu diwaspadai dan perlu diberikan perhatian penuh agar kejahatan ini tidak terus mewabah serta mengakibatkan kerugian besar bagi instansi terkait dan penggunanya. Maka dari itu, urgensi pembentukan Undang-undang terkait dengan keamanan keuangan siber perlu dirancang untuk dapat melindungi pertahanan sistem finansial di sektor keuangan. Dari pemaparan tersebut maka dapat diambil beberapa point permasalahan yang akan dibahas yakni sebagai berikut :

1. Bagaimana regulasi hukum Indonesia dalam memandang permasalahan kejahatan keuangan siber ini?
2. Apa yang harus dilakukan pemerintah, aparat yang berwajib dan masyarakat dalam memerangi kejahatan keuangan siber ini?
3. Apa sanksi yang pantas diberikan bagi para penjahat keuangan siber?

2. METODE PENELITIAN

Jenis penelitian ini merupakan penelitian yuridis normatif yang berfokus pada peraturan perundang undangan yang terkait dengan fokus penelitian penulis. Penelitian jenis ini bertujuan untuk mengkaji hukum sebagai aturan yang bersifat tertulis. Adapun yang dipergunakan sebagai bahan hukum primer dalam penelitian ini adalah Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK), Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Peraturan Jasa Otoritas Keuangan Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, POJK Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan serta ahan hukum sekunder yang digunakan dalam penelitian ini yakni Buku-Buku hukum serta jurnal penelitian hukum dengan menggunakan pendekatan teoritis untuk dapat menganalisa peraturan hukum yang berlaku.

3. HASIL DAN PEMBAHASAN

Regulasi Hukum Indonesia dalam Memandang Permasalahan Kejahatan Keuangan Siber

Keamanan digital yang juga kerap kali disebut dengan keamanan siber merupakan suatu konsep perlindungan aset dan informasi digital yang dimiliki oleh penggunanya. Keamanan digital ini mencangkup berbagai aspek seperti sistem digital seperti komputer dan jaringan dari tindak kejahatan penyadapan, pencurian, kerusakan serta mempertahankan kerahasiaan data diri pribadi agar tidak disalahgunakan pihak yang tidak bertanggung jawab termasuk hal nya perusahaan. Serangan siber ini kerap kali terjadi ketika seseorang berusaha menganggu sistem secara logis dan fisik untuk dapat merusak kerahasiaan, integritas serta ketersediaan informasi yang ada (Cloudmatika.co, 2022).

Maka dari itu, keamanan digital sangatlah penting karena kejahatan siber yang marak terjadi saat ini yakni seperti *phising*, *malware*, ataupun serangan lain yang fokusnya untuk dapat mencuri informasi keuangan, akses rekening bank, pengendalian sistem keuangan secara menyeluruh serta pencurian dan pemanfaatan data diri pengguna untuk hal lain menjadi permasalahan utama yang mengintai kehidupan masyarakat. terdapat beberapa cara yang dapat dilakukan untuk dapat melindungi sistem keuangan siber ini seperti penggunaan teknologi keamanan tingkat tinggi, peningkatan kesadaran pengguna dan adopsi praktik keamanan digital yang kuat, dengan hal ini maka setidaknya dapat mengurangi angka kebocoran data informasi dan keuangan pengguna dan memastikan keamanan sistem (Putri et al., 2023).

Regulasi ataupun peraturan hukum Indonesia sangat diperlukan dalam menangani permasalahan ini karena pada dasarnya masih kaburnya peraturan khusus yang mengatur terkait dengan keamanan keuangan digital. Terdapat beberapa penguatan mengapa peraturan ini sangat dibutuhkan yakni karena saat ini manusia hidup berdampingan dengan berkembangnya teknologi yang sangat pesat, semakin pesat perkembangan teknologi maka kesempatan melakukan kejahatan di dunia siber inipun tidak menutup kemungkinan akan semakin terbuka lebar. Kemudian perlindungan untuk para konsumen juga belum maksimal karena masih marak ditemui kasus penipuan berbasis siber yang banyak menyebabkan kerugian besar bagi konsumen terutama dalam kerugian materil serta melemahnya regulasi eksisting, meskipun banyak terdapat peraturan hukum yang secara eksplisit mengatur terkait dengan perlindungan data konsumen *Fintech,* teknologi *blockchain* dan sebagainya seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perbankan, Undang-Undang Tindak Pidana Pencucian Uang sama sekali belum menjawab keresahan masyarakat terkait dengan kejahatan di dalam ranah keuangan siber. Pendekatan ini dinilai kurang efektif karena regulasi tersebut tidak terfokus dalam menangani kejahatan keuangan siber ini ditambah dengan belum ada mekanisme pengaduan dan ganti rugi yang tersedia bagi konsumen yang menjadi korban kejahatan siber. Terdapat beberapa negara di dunia yang telah membentuk regulasi keamanan keuangan siber ini seperti Amerika Serikat dalam *Gram-Leach-Bliley Act* (GLBA) dan *Cybersecurity Information Sharing Act* (CISA) yang memfokuskan pada perlindungan data konsumen dan kolaborasi aktif dalam sektor publik-swasta untuk mendeteksi adanya ancaman secara real-time (Yang A et al., 2020). Kemudian Singapura juga membuat peraturan yang mewajibkan pelaporan insiden siber secara cepat melalui *Cyberscurity Act* serta panduan teknis dari *Monetary Authority of Singapore* (MAS) untuk dapat melakukan pengelolaan risiko teknologi dalam lembaga keuangan (Fuda, 2025).

Peran Pemerintah, Aparat Berwajib serta Masyarakat dalam Memerangi Kejahatan Keuangan Siber

Dewasa ini, risiko penggunaan keuangan secara digital atau siber semakin hari semakin meningkat dan memberikan efek paranoid bagi pada penggunanya. Kejahtaan siber yang telah merajah di era modern seperti saat ini merupakan suatu bukti bahwasanya negara Indonesia memang membutuhkan payung hukum yang mengatur secara khsusus terkait dengan ancaman ini. Dalam konteks keamanan keuangan siber, keamanan digital menjadi sangat penting untuk diutamakan karena keamanan digital yang baik maka akan meminimalisir terjadinya kasus kasus serangan siber berupa phising, malware atau serangan lainnya yang dapat berdampak pada tercurinya informasi keuangan, akses rekening bank oleh orang yang tidak

bertanggungjawab atau bakan pengendalian sistem keuangan korban secara keseluruhan. Maka dari itu, peningkatan keamanan digital, penguatan peran pemerintah dan aparat berwajib serta kesadaran pengguna menjadi pondasi pembentukan keuangan siber yang aman.

Peningkatan keamanan digital memainkan peranan yang sangat krusial dalam menjaga keamanan keuangan siber terutama pada era digital yang semakin hari semakin berkembang ini. Khususnya peningkatan keamanan pada aplikasi *fintech* yang mana *fintech* ini merupakan penggabungan teknologi dengan layanan keuangan untuk dapat menciptakan solusi baru bagi manusia yang lebih efisien dan efektif contohnya yakni pada mobile-banking, dompet digital dan teknologi *blockchain* dalam transaksi keuangan (Qur'anisa, 2024).

Meskipun efisien, risiko keamanan data dan transaksi akan lebih besar karena pengguanaan teknologi dalam pengaplikasiannya. Untuk itu sejalan dengan Undang-undang Perlindungan Data Pribadi beberapa cara yang dapat ditempuh untuk dapat meningkatkan keamanan digital pada keuangan siber ini yakni dengan cara menerapkan enkripsi data dengan menggunakan protokol enkripsi end-to-end untuk dapat melindungi data konsumen dari aktivitas ilegal selama transmisi dan penyimpanan. Pengenaan autentikasi multi-faktor (MFA) menjadi kewajiban untuk dapat memastikan identitas pengguna yang diyakini sah sebagaimana yang telah diatur dalam Pasal 35 ayat (1) Undang-undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi yang berbunyi *"Pengendalian data pribadi wajib melakukan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan perlindungan data pribadi dari pemrosesan yang melanggar hukum."*

Selain peningkatan keamanan digital peranan pemerintah juga sangat dibutuhkan karena sejatinya pemerintah memiliki tanggungjawab besar dalam hal ini mengingat perannya sebagai pembentuk regulasi untuk kepentingan masyarakat luas. Meskipun telah terbentuk Undang Undang Informasi dan Transaksi Elektronik di Indonesia akan tetapi pada realitanya dunia siber tetaplah sulit untuk dapat dijinakan (Setiawan, 2013). Apalagi UU ITE pada dasarnya tidak mengatur secara terperinci mengenai keamanan keuangan siber yang dapat menyebabkan celah yang bisa dimanfaatkan bagi para penjahat keuangan siber dalam melancarkan aksinya. Maka dari itu, perlu bagi pemerintah sebagai regulator untuk membentuk regulasi baru demi menjawab keresahan masyarakat terkait dengan keamanan keuangan siber, pembentukan ini harus berlandaskan pada kerangka hukum yang kuat.

Selain membentuk undang-undang baru pemerintah juga diharapkan dapat melakukan pengawasan secara berkala melalui lembaga Otoritas Jasa Keuangan dan Bank Indonesia serta menerapkan standar operasional keamanan untuk sektor keuangan tersebut untuk dapat meminimalisir adanya celah dan risiko dengan cara menghimbau pengusaha Fintech serta

perbankan melakukan pelaporan secara rutin serta mematuhi setiap regulasi yang disahkan. Pemerintah juga harus melaksanakan kolaborasi dengan aparat berwajib agar tetap dapat mempertahankan ekosistem keuangan digital yang aman (Hasanah et al., 2024). Dalam kolaborasi tersebut mengharuskan adanya infrastruktur yang mampu mendeteksi ancaman siber secara tanggap, menetapkan standar keamanan teknologi yang tinggi serta mengajak masyarakat berpartisipasi aktif dalam menjaga keamanan keuangan siber ini. Masyarakat hendaklah lebih aware dalam melakukan sesuatu terkait dengan keuangan digital, masyarakat haruslah sekurang kurangnya dapat diberikan pelatihan terkait dengan bagaimana cara menjaga keamanan akun keuangan digital oleh para penyedia jasa keuangan seperti fintech tersebut, dengan upaya upaya tersebut maka sistem keuangan digital akan terjamin keamanannya serta meminimalisir adanya kerugian yang ditimbulkan oleh pihak-pihak yang tidak bertanggung jawab.

Sanksi yang Wajib Diberlakukan untuk Pelaku Kejahatan Keamanan Keuangan Siber

Sanksi merupakan suatu hukuman atas perbuatan seseorang yang melawan hukum yang mana perbuatan tersebut dapat dibuktikan bersalah menurut hukum (Mathar, 2023). Dalam pemberian sanksi bagi pelaku tindak kejahatan keuangan siber haruslah sesuai dengan kerugian yang ditimbulkan serta dapat memberikan efek jera pada pelaku sekaligus dapat melindungi sistem keuangan serta meminimalisir terjadinya tindak kejahatan yang sama. Beberapa sanksi yang dapat diterapkan bagi para pelaku kejatahan ini yakni sebagai berikut, yakni Saksi pidana yang dalam hal ini dibentuk khusus untuk dapat memberikan efek jera bagi pelaku. Sanksi pidana yang relevan yang bisa diterapkan serta dapat dijadikan bahan untuk pembentukan peraturan atau regulasi baru terkait dengan tindak pidana keuangan siber ini yakni Pasal 30 Ayat (3) Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi *"Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)."*

Selain sanksi pidana, pelaku tindak kejahatan penyerangan keamanan keuangan siber ini juga layak diberikan sanksi secara perdata karena pelaku menyebabkan kerugian materil bagi para korbannya dengan cara memberikan ganti rugi atas kerugian yang telah ditimbulkan oleh pelaku. Dengan penerapan sanksi tersebut maka para pelaku akan mendapatkan efek jera dan juga sebagai tindakan prefentif agar tidak ada lagi oknum-oknum nakal yang melakukan hal tersebut.

4. KESIMPULAN

Keamanan keuangan siber merupakan aspek utama yang harus menjadi fokus perhatian lebih bagi pemerintah, penyedia jasa dan masyarakat. Hampir setengah dari kehidupan manusia saat ini telah didominasi oleh teknologi yang artinya semakin berpengaruh teknologi dalam aspek kehidupan maka semakin besar pula risiko yang akan dihasilkan. Maka dari itu, untuk dapat meminimalisir terjadinya risiko teknologi ini maka terdapat beberapa tindakan preventif yang harus dilakukan oleh seluruh lapisan masyarakat, apalagi dalam pengaplikasian teknologi dalam sektor keuangan. Penggabungan antara teknologi dan keuangan ini merupakan suatu solusi bagi manusia yang dapat mempermudah hampir 70% kegiatan transaksi dengan melalui keuangan digital ini. Di Indonesian belum terdapat payung hukum yang mampu menaungi keamanan keuangan siber ini, meskipun masih banyak peraturan perundang undangan yang mengatur tentang teknologi akan tetapi peraturan khusus untuk keamanan keuangan siber ini tetap diperlukan agar bahasan dan regulasi yang dihasilkan bersifat tegas, jelas dan nyata. Jika negara ini belum memiliki regulasi terkait dengan keamanan keuangan siber tersebut maka akan banyak menimbulkan celah bagi para oknum untuk dapat melancarkan aksinya, akibatnya banyak orang yang mengalami kerugian terutama dalam kerugian materil. Maka dari itu, urgensi pembentukan undang undang keamanan keuangan siber adalah sepenuhnya dilakukan untuk melindungi sistem finansial di sektor digital.

DAFTAR REFERENSI

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. *Akuntansi dan Teknologi Informasi*, *17*(2), 221-237.

Cloudmatika.co. (2022). Apa Itu Keamanan Digital.

Fuda, K. (2025). The evolution of financial regulation and the role of the monetary authority of Singapore: a historical analysis based on organizational knowledge creation theory. *Management & Organizational History*, *20*(1), 130-152.

Hasanah, N., Sayuti, M. N., & Lisnawati, L. (2024). Optimalisasi regulasi perbankan syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam akselerasi transformasi digital. *Jurnal Manajemen Terapan Dan Keuangan*, *13*(03), 709-723.

Qur'anisa, Z., Herawati, M., Lisvi, L., Putri, M. H., & Feriyanto, O. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital: Studi Literatur. *GEMILANG: Jurnal Manajemen Dan Akuntansi*, *4*(3), 99-114.

Mathar, A. (2023). Sanksi Dalam Peraturan Perundang-Undangan. *'Aainul Haq: Jurnal Hukum Keluarga Islam*, *3*(II).

Setiawan, R., & Arista, M. O. (2013). Efektivitas undang-undang informasi dan transaksi elektronik di indonesia dalam aspek hukum pidana. *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, *2*(2).

Putri, A. A., & Yusuf, H. (2025). Ransomware di sektor keuangan: Studi kasus serangan terhadap BSI pada tahun 2023. *Jurnal Intelek Insan Cendikia*, *2*(8), 15649-15656.

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173-181.

Yang, A., Kwon, Y. J., & Lee, S. Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777-1794.

Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan (Lembar Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253)

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Lembar Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820)

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembar Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905)

Peraturan Otoritas Jasa Keuangan Pojk Nomor 40 Tahun 2024 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 53/Ojk, Tambahan Lembaran Negara Republik Indonesia Nomor 121/Ojk)

POJK Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan