Juris Sinergi Journal (JSJ)
Volume I; Number I; Month 5, Year 2024
Doi : -
Website : https://sinergilp.com
E-ISSN : 3048-4308

Tinjauan Hukum terhadap Kejahatan Siber dalam Transaksi Financial Technology

Ayumi Kartika Sari
Universitas Prima Indonesia
ayumikartikasari@unprimdn.ac.id

Abstrak

Kejahatan siber dalam transaksi Financial Technology (Fintech) adalah salah satu tantangan hukum yang signifikan di era digital. Dengan berkembangnya teknologi, transaksi keuangan semakin beralih ke platform digital, dan ini menciptakan peluang baru bagi para pelaku kejahatan siber. Kejahatan dunia maya mengacu pada tindakan ilegal yang menggunakan komputer atau internet . Beberapa contoh kejahatan dunia maya antara lain: Mencuri dan menjual data perusahaan. Menuntut pembayaran untuk mencegah serangan. Menginstal virus pada komputer target. Hukum financial technology (fintech) adalah seperangkat peraturan dan undang-undang yang mengatur operasional dan aktivitas dari perusahaan fintech. Ini mencakup segala aspek hukum yang relevan dengan layanan keuangan berbasis teknologi, seperti pembayaran digital, pinjaman online, investasi, dan asuransi berbasis teknologi. Di Indonesia, hukum fintech diatur oleh beberapa lembaga, termasuk Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), yang mengeluarkan peraturan terkait pendaftaran, perizinan, pengawasan, dan perlindungan konsumen untuk perusahaan fintech.

Kata Kunci: Hukum; Kejahatan Ciber; Financial Technologi.

PENDAHULUAN

Pesatnya perkembangan teknologi digital telah mempengaruhi berbagai sektor, termasuk sektor keuangan. Financial Technology (Fintech) muncul sebagai inovasi dalam layanan keuangan, memungkinkan transaksi menjadi lebih mudah, cepat, dan efisien. Namun, perkembangan ini juga menimbulkan tantangan baru, termasuk peningkatan risiko kejahatan siber. Dalam beberapa tahun terakhir, sektor FinTech telah berkembang pesat, memudahkan transaksi keuangan digital, pinjaman online, pembayaran mobile, dan layanan keuangan lainnya. Kemudahan ini sejalan dengan meningkatnya risiko kejahatan siber yang menargetkan sistem-sistem ini.

Platform FinTech sering menjadi target kejahatan siber karena mereka menyimpan data keuangan dan pribadi pengguna dalam jumlah besar. Serangan siber seperti hacking, phishing, dan malware dapat menyebabkan kerugian finansial yang signifikan, baik bagi individu maupun perusahaan. Kejahatan siber merujuk pada tindakan ilegal yang dilakukan melalui teknologi informasi dan internet. Dalam konteks Fintech, kejahatan siber dapat mencakup pencurian data, penipuan digital, peretasan sistem keuangan, hingga penyalahgunaan informasi pribadi dan keuangan. Kejahatan ini berpotensi merugikan tidak hanya perusahaan Fintech, tetapi juga konsumen dan integritas sistem keuangan secara keseluruhan.

Dengan berkembangnya FinTech, diperlukan kerangka hukum yang kuat untuk melindungi konsumen dan menjaga integritas sistem keuangan. Tinjauan hukum terhadap kejahatan siber dalam FinTech membantu memahami bagaimana regulasi saat ini mengatasi ancaman ini dan apa yang perlu diperbaiki. Meningkatnya ancaman kejahatan siber dalam transaksi Fintech, regulasi hukum yang efektif menjadi sangat penting. Regulasi ini harus mampu mengimbangi

perkembangan teknologi dan memberikan perlindungan hukum yang memadai bagi semua pihak yang terlibat dalam ekosistem Fintech.

Meskipun beberapa negara telah mengadopsi regulasi terkait keamanan siber dan perlindungan data, implementasi dan penegakan hukum tetap menjadi tantangan. Peraturan hukum harus dapat beradaptasi dengan cepat terhadap perubahan teknologi, sementara penegakan hukum perlu dilakukan secara konsisten dan efektif untuk mencegah dan menindak kejahatan siber. Kejahatan siber dalam transaksi FinTech dapat menyebabkan kerugian besar bagi konsumen, termasuk pencurian identitas dan hilangnya dana. Latar belakang ini penting untuk menekankan perlunya regulasi yang melindungi konsumen dari risiko-risiko ini.

Kejahatan siber yang menargetkan sektor FinTech dapat memiliki dampak ekonomi yang luas, baik dalam hal kerugian langsung maupun kepercayaan publik terhadap teknologi keuangan. Ini juga mempengaruhi stabilitas pasar keuangan yang lebih luas. Selain regulasi, kesadaran akan risiko kejahatan siber dan pentingnya keamanan digital harus ditingkatkan di kalangan pelaku industri Fintech dan masyarakat umum. Edukasi mengenai praktik keamanan yang baik dan perlindungan data pribadi menjadi kunci dalam mencegah kejahatan siber.

Dalam konteks global, berbagai negara memiliki regulasi yang berbeda terkait dengan FinTech dan keamanan siber. Tinjauan hukum dapat memberikan wawasan tentang praktik terbaik di tingkat internasional dan bagaimana Indonesia dapat menyesuaikan regulasinya untuk memenuhi standar global. Sementara inovasi di bidang FinTech menawarkan berbagai manfaat, mereka juga membawa risiko baru. Penting untuk meninjau bagaimana hukum dapat mengikuti perkembangan teknologi dan menjaga keseimbangan antara inovasi dan keamanan.

Latar belakang ini memberikan dasar untuk memahami pentingnya kajian hukum terhadap kejahatan siber dalam FinTech dan bagaimana regulasi dapat berkembang untuk menghadapi tantangan ini. Melalui kajian hukum ini, diharapkan dapat ditemukan solusi dan rekomendasi yang efektif untuk memitigasi risiko kejahatan siber dalam transaksi Fintech serta memperkuat kerangka hukum yang ada.

METODE

Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundangundangan terkait cyber-crime. Metode pengumpulan data dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain. Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan cyber law di Indonesia.

Pendekatan yang dipergunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Penulis mengkaji Undang-Undang mengenai cyber law sedangkan Bahan Hukum yang dipergunakan adalah bahan hokum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundangundangan yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.

HASIL DAN PEMBAHASAN

Tantangan Hukum dalam Penanganan Kejahatan Siber di FinTech

Kejelasan Regulasi : Banyak negara, termasuk Indonesia, masih dalam tahap awal pengembangan regulasi terkait FinTech dan kejahatan siber. Meskipun beberapa undang-

undang telah diadaptasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, namun belum sepenuhnya mengakomodasi kompleksitas kejahatan siber di sektor ini.

Jurisdiksi Lintas Negara : Kejahatan siber sering kali melibatkan pelaku yang berada di yurisdiksi berbeda dengan korban atau platform yang diserang, sehingga menimbulkan tantangan dalam penegakan hukum lintas negara.

Kejahatan Siber yang Umum Terjadi dalam Transaksi FinTech

Phishing dan Social Engineering : Ini merupakan metode yang sering digunakan untuk mencuri data pribadi pengguna, seperti informasi login atau data kartu kredit, dengan menyamar sebagai entitas tepercaya.

Malware dan Ransomware : Malware dapat diinstal pada perangkat pengguna tanpa sepengetahuan mereka, memungkinkan pencurian informasi atau kontrol terhadap perangkat tersebut. Ransomware, di sisi lain, mengunci akses pengguna ke perangkat atau data mereka sampai tebusan dibayar.

Fraud dalam Pembayaran : Penipuan melalui transaksi palsu atau pencurian identitas untuk melakukan transaksi tanpa sepengetahuan pemilik akun juga merupakan masalah besar dalam sektor FinTech.

Peran Pemerintah dan Otoritas dalam Mengatasi Kejahatan Siber

Penguatan Regulasi dan Kerangka Hukum : Pemerintah perlu memperbarui dan memperkuat kerangka hukum untuk mengatasi kejahatan siber yang semakin canggih, termasuk regulasi khusus untuk sektor FinTech. Kolaborasi dengan otoritas global juga penting untuk menangani kejahatan yang melibatkan lebih dari satu yurisdiksi.

Edukasi dan Kesadaran Pengguna : Kampanye edukasi yang menargetkan pengguna tentang bahaya kejahatan siber dan cara melindungi diri mereka sendiri merupakan langkah penting dalam mencegah serangan.

Teknologi dan Inovasi dalam Menghadapi Kejahatan Siber

Penggunaan Teknologi Keamanan Canggih : FinTech harus mengadopsi teknologi keamanan yang lebih canggih seperti enkripsi end-to-end, autentikasi multi-faktor, dan kecerdasan buatan untuk mendeteksi anomali dalam transaksi.

Kerjasama dengan Pihak Ketiga : Platform FinTech dapat bekerja sama dengan perusahaan keamanan siber untuk memperkuat infrastruktur mereka terhadap potensi serangan.

Pembahasan dalam era digital saat ini, Financial Technology (FinTech) telah menjadi bagian penting dari kehidupan sehari-hari, memungkinkan transaksi yang lebih mudah, cepat, dan efisien. Namun, di balik inovasi ini, terdapat ancaman yang signifikan dari kejahatan siber yang dapat merusak integritas dan kepercayaan terhadap sistem FinTech.

Regulasi yang Belum Optimal : Meskipun telah ada upaya untuk mengatur FinTech dan melindungi konsumen dari kejahatan siber, regulasi yang ada masih kurang memadai. Misalnya, UU ITE di Indonesia tidak secara khusus mengatur sektor FinTech, sehingga penegakan hukum sering kali menemui kesulitan dalam menindak kejahatan siber yang terjadi di sektor ini.

Tantangan Lintas Negara : Kejahatan siber sering kali melibatkan pelaku yang beroperasi dari berbagai negara, yang menambah kerumitan dalam proses penegakan hukum. Perjanjian internasional dan kerjasama antara negara-negara menjadi sangat penting untuk menangani kasus-kasus ini.

Peran Teknologi dalam Pencegahan : Adopsi teknologi keamanan yang lebih canggih menjadi kebutuhan mendesak bagi platform FinTech. Penggunaan kecerdasan buatan untuk mendeteksi dan merespon ancaman siber secara real-time merupakan salah satu pendekatan yang efektif dalam melindungi transaksi online.

Kejahatan siber dalam konteks financial technology (fintech) merupakan salah satu tantangan besar dalam perkembangan teknologi finansial modern. Tinjauan hukum terhadap kejahatan siber ini perlu dilakukan untuk memastikan keamanan transaksi serta perlindungan konsumen. Berikut adalah pembahasan mengenai hal tersebut:

Definisi Kejahatan Siber dalam Fintech

Kejahatan siber dalam transaksi fintech merujuk pada tindakan ilegal yang dilakukan melalui teknologi digital dengan tujuan mencuri data, uang, atau mengganggu sistem keuangan. Contoh kejahatan ini termasuk pencurian identitas, hacking, phishing, serta penyalahgunaan data.

Kejahatan siber dalam fintech merujuk pada segala bentuk tindakan kriminal yang menggunakan teknologi digital atau jaringan komputer untuk menyerang, mengakses, mencuri, atau memanipulasi data, sistem, atau aset keuangan yang dikelola oleh perusahaan finansial teknologi (fintech). Kejahatan ini dapat mencakup berbagai bentuk serangan, seperti:

1. **Phishing**: Penipuan melalui email, pesan, atau situs web palsu yang bertujuan untuk mendapatkan informasi pribadi atau keuangan dari korban.
2. **Malware**: Penggunaan perangkat lunak berbahaya untuk menginfeksi sistem komputer fintech, yang dapat mencuri data, mengganggu operasi, atau mengakses informasi sensitif.
3. **Ransomware**: Serangan yang mengenkripsi data perusahaan fintech dan menuntut tebusan untuk memulihkan akses.
4. **Penipuan Identitas**: Penggunaan identitas palsu atau curian untuk mengakses layanan keuangan atau melakukan transaksi ilegal.
5. **Serangan DDoS (Distributed Denial of Service)**: Serangan yang membanjiri server fintech dengan lalu lintas palsu untuk membuat layanan tidak tersedia bagi pengguna yang sah.
6. **Hacking**: Akses tidak sah ke sistem atau jaringan fintech untuk mencuri data, uang, atau merusak operasi perusahaan.

Kejahatan siber dalam fintech sangat merugikan, tidak hanya dari segi finansial tetapi juga dari sisi kepercayaan pelanggan, integritas data, dan reputasi perusahaan. Oleh karena itu, fintech harus menerapkan langkah-langkah keamanan yang ketat untuk melindungi diri dari ancaman ini.

Regulasi dan Perlindungan Hukum

Setiap negara memiliki regulasi yang berbeda terkait keamanan siber, namun beberapa prinsip dasar tetap berlaku, seperti:

- **Perlindungan Data Pribadi**: Regulasi seperti GDPR di Eropa atau UU ITE dan Peraturan Perlindungan Data Pribadi di Indonesia menekankan pentingnya menjaga kerahasiaan dan integritas data konsumen.

- **Keamanan Sistem**: Penyedia layanan fintech diwajibkan menerapkan sistem keamanan yang kuat, termasuk enkripsi dan autentikasi ganda, untuk mencegah akses tidak sah.
- **Tanggung Jawab Hukum**: Pengaturan hukum juga mencakup tanggung jawab penyedia layanan fintech terhadap kerugian yang dialami konsumen akibat kejahatan siber.

Tantangan dalam Penegakan Hukum

- **Jurisdiksi**: Kejahatan siber seringkali lintas negara, sehingga penegakan hukum menjadi lebih kompleks karena melibatkan berbagai yurisdiksi.
- **Evolusi Teknologi**: Teknologi yang terus berkembang menuntut regulasi dan penegakan hukum yang adaptif. Peraturan yang ada seringkali tertinggal dibandingkan dengan kemajuan teknologi.
- **Bukti Digital**: Pengumpulan dan pembuktian dalam kasus kejahatan siber memerlukan teknik forensik digital yang canggih, yang tidak selalu tersedia di semua yurisdiksi.

Upaya Pencegahan dan Penegakan Hukum

- **Kolaborasi Internasional**: Mengingat kejahatan siber sering melibatkan pelaku dari berbagai negara, kolaborasi internasional melalui organisasi seperti Interpol menjadi krusial.
- **Edukasi dan Kesadaran**: Meningkatkan kesadaran konsumen dan perusahaan tentang risiko kejahatan siber dan cara pencegahannya sangat penting.
- **Peningkatan Kapasitas Penegak Hukum**: Penegak hukum perlu dilatih dan diberdayakan dengan teknologi serta pengetahuan terbaru untuk menghadapi kejahatan siber.

Penegakan hukum dalam kasus kejahatan siber di sektor fintech adalah aspek krusial dalam melindungi integritas sistem keuangan digital, serta menjaga kepercayaan konsumen dan integritas industri keuangan itu sendiri. Berikut adalah beberapa poin penting mengenai penegakan hukum dalam konteks ini:

1. Regulasi dan Kerangka Hukum

- **Regulasi Spesifik:** Negara-negara biasanya memiliki regulasi khusus yang mengatur industri fintech dan keamanan sibernya. Di Indonesia, misalnya, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia memiliki peraturan yang mengatur perlindungan data dan keamanan transaksi dalam sektor fintech.
- **Undang-Undang ITE:** Di Indonesia, penegakan hukum terhadap kejahatan siber umumnya mengacu pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ini memberikan dasar hukum untuk menindak pelaku kejahatan siber yang menyalahgunakan teknologi informasi.

2. Kerjasama Antar Lembaga

- **Polri dan OJK:** Dalam menangani kejahatan siber di fintech, seringkali terdapat kerjasama antara kepolisian (Polri) dengan OJK atau BI. Kerjasama ini meliputi pertukaran informasi, pelatihan, serta operasi gabungan untuk mengidentifikasi dan menindak pelaku kejahatan.

- **Internasional:** Mengingat kejahatan siber seringkali bersifat lintas negara, kerjasama internasional juga diperlukan. Ini termasuk pertukaran informasi dan koordinasi dengan lembaga penegak hukum di negara lain serta organisasi internasional seperti Interpol.

3. Teknologi dan Metode Penegakan Hukum

- **Digital Forensics:** Teknologi forensik digital digunakan untuk mengumpulkan bukti dari perangkat digital yang digunakan oleh pelaku kejahatan. Ini mencakup analisis perangkat lunak, jejak digital, dan rekaman transaksi.
- **Cybersecurity Measures:** Penegakan hukum juga mencakup penerapan langkah-langkah keamanan siber di dalam perusahaan fintech itu sendiri, seperti enkripsi data, autentikasi multi-faktor, dan pemantauan aktivitas yang mencurigakan.

4. Sanksi dan Hukuman

- **Pidana:** Pelaku kejahatan siber dapat dikenai sanksi pidana, termasuk penjara dan denda yang besar, tergantung pada jenis dan tingkat kejahatannya.
- **Sanksi Administratif:** Selain hukuman pidana, pelanggaran dalam sektor fintech juga dapat dikenai sanksi administratif oleh otoritas terkait, seperti pencabutan izin operasi atau denda administratif.

5. Perlindungan Konsumen

- **Mekanisme Pengaduan:** Konsumen yang menjadi korban kejahatan siber di sektor fintech harus memiliki akses ke mekanisme pengaduan yang efektif dan perlindungan hukum.
- **Restitusi dan Kompensasi:** Bagian dari penegakan hukum adalah memastikan bahwa korban kejahatan siber mendapatkan ganti rugi yang adil.

6. Peningkatan Kapasitas

- **Pelatihan dan Pendidikan:** Aparat penegak hukum harus mendapatkan pelatihan yang memadai dalam teknologi digital dan metodologi terbaru dalam penanganan kejahatan siber.
- **Awareness Campaigns:** Edukasi kepada masyarakat tentang risiko kejahatan siber dan cara pencegahannya juga merupakan bagian penting dari penegakan hukum.

Dalam menghadapi kejahatan siber di sektor fintech, penegakan hukum harus bersifat proaktif, responsif, dan adaptif terhadap perkembangan teknologi dan modus operandi yang digunakan oleh pelaku kejahatan.

Studi kasus dan preseden hukum memberikan gambaran mengenai bagaimana sistem peradilan menangani kejahatan siber di bidang fintech. Ini juga membantu dalam memperbaiki regulasi dan strategi penegakan hukum di masa depan. Regulasi yang ada perlu diperbaharui secara berkala untuk menyesuaikan dengan perkembangan teknologi dan modus kejahatan siber. Kerjasama antara pemerintah, penyedia

layanan fintech, dan institusi keuangan penting untuk menciptakan ekosistem yang lebih aman

KESIMPULAN

Penanganan kejahatan siber dalam transaksi FinTech memerlukan pendekatan holistik yang mencakup penguatan regulasi, edukasi pengguna, adopsi teknologi keamanan canggih, serta kerjasama lintas negara. Tanpa langkah-langkah ini, risiko terhadap pengguna dan penyedia layanan FinTech akan terus meningkat seiring dengan pertumbuhan sektor ini. Tinjauan hukum terhadap kejahatan siber dalam transaksi fintech merupakan langkah penting untuk memastikan keamanan dan kepercayaan dalam penggunaan teknologi finansial. Regulasi yang kuat, penegakan hukum yang efektif, serta kolaborasi berbagai pihak menjadi kunci utama dalam menghadapi tantangan ini.

DAFTAR PUSTAKA

Abubakar, L., & Handayani, T., 'Financial Technology: Legal Challenges for Indonesia Financial Sector' (2018)175 IOP Publishing.

Arief, Nawawi B., 'Kebijakan Penanggulangan Cyber Crime dan Cyber Sex' (2006) 1 Law Reform.

Abdul Agis, Peranan Kepolisian Dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronik, Jurnal Al hikam, Vol. 1No. 2, 2017.

Asari, Dakum dan Aang, 'Urgensi Pembentukan Undang-Undang Fintech sebagai Upaya Legalisasi Penyelesaian Sengketa Transaksi Fintech di Indonesia', (2020) 2 Jurnal Borobudur Law Review

Budi Kristian Rivanda Putra, Kebijakan Aplikasi Tindak Pidana Siber Di Indonesia, Journal of law, Vol. 1, 2018

Dwila Annisa & Mujiono Hafidh, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism, Jurnal Pembangunan Hukum Indonesia, Vol. 3 No. 2, 2021

Marginingsih, Ratnawaty, 'Analisis SWOT Technology Financial (FinTech) Terhadap Industri Perbankan', (2019), (19), Cakrawala-Jurnal Humaniora Bina Sarana Informatika.

Njatrijani, 'Perkembangan Regulasi dan Pengawasan Financial',(2019) 4 Jurnal Diponegoro Private Law.

Nabila, F. (2019). Mengenal Jenis-Jenis Financial Technology. https://smartlegal.id/smarticle/2019/01/08/mengenal-jenis-jenis-financialtechnology/, Diakses 20 Juni 2021.

Njatrijani, R. (2019). Perkembangan Regulasi Dan Pengawasan Financial Technologydi Indonesia. Diponegoro Private Law Review, 4(1).

Noor, A., & Wulandari, D. (2021). Landasan Konstitusional Perlindungan Data Pribadi Pada Transaksi Fintech Lending di Indonesia. Jurnal Ilmiah Dunia Hukum, 99-110.

Novinna, V. (2020). Perlindungan Konsumen dari Penyebarluasan Data Pribadi oleh Pihak Ketiga: Kasus Fintech "Peer to Peer Lending". Jurnal Magister Hukum Udayana, 9(1), 92-110

Situmeang, Sahat Maruli Tua (2021), Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber, Jurnal SAS1I (1), 38 – 52

Sitompul, Meline Gerarita, 'Urgensi Legalitas Financial Technology (Fintech) : Peer to Peer (P2P) Lending di Indonesia', (2018) 1 Jurnal Yuridis Unaja.

Stevani dan Sudirman, ‘Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia’, (2021) 2 Jurnal Universitas Internasional Batam.