Jurist-Diction
Volume 6 No. 4, Oktober 2023

Perlindungan Hukum atas Tindakan Pencurian Data Pribadi pada Layanan Fintech Lending Terhadap Ancaman Cyber Security di Indonesia

Amiliya Handayani
amiliya.handayani@gmail.com
Universitas Airlangga

How to cite:
Amiliya Handayani, 'Perlindungan Hukum atas Tindakan Pencurian Data Pribadi pada Layanan Fintech Lending Terhadap Ancaman Cyber Security di Indonesia' (2023) Vol. 6 No. 4 Jurist-Diction

Histori artikel:
Submit 25 Mei 2023;
Diterima 17 Juni 2023;
Diterbitkan 30 Oktober 2023.

DOI:

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract

This research will answer all form of cyber security threats to fintech lending services in Indonesia as well as parties who are responsible for victims of personal data theft on fintech lending services in Indonesia. The approach method used in this research is the statutory approach and the conceptual approach. The exixtence of fintech lending makes it easy for people to make loans online easily and quickly. This makes fintech lending services providers faced with cyber security threats, therefore it is necessary to maximize the system and its operation. Judging from several regulations related to identity theft in fintech lending services, there are several perspectives that require the protection of personal data. In the event of data leakage or theft, users of fintech lending services who are disadvantaged can take legal remidies in the form of non-yudicial legal remidies and judicial legal remidies.

Keywords: Personal Data Protection; Cyber Security; Fintech Lending.

Abstrak

Dalam penelitian ini akan menganalisis tentang bentuk ancaman cyber security pada layanan fintech lending di Indonesia serta pihak yang bertanggung gugat terhadap korban pencurian data pribadi pada layanan fintech lending di Indonesia. Metode pendekatan yang digunakan dalam penelitian ini adalah Pendekatan perundang-undangan (Statute Approach) dan Pendekatan Konseptual (Conceptual Approach). Adanya fintech lending memberikan kemudahan bagi masyarakat dalam melakukan pinjaman secara online dengan mudah dan cepat. Hal tersebut membuat penyelenggara layanan fintech lending dihadapkan pada ancamaan cyber security, oleh karena itu perlu untuk memaksimalkan sistem serta pengoperasiannya. Ditinjau dari beberapa regulasi terkait pencurian identitas pada layanan fintech lending, terdapat beberapa perspektif yang mengharuskan dilakukannya perlindungan data pribadi. Dalam hal kebocoran maupun pencurian data, maka pengguna layanan fintech lending yang dirugikan dapat melakukan upaya hukum berupa upaya hukum non – yudisial dan upaya hukum yudisial

Kata Kunci: Perlindungan Data Pribadi; Cyber Security; Fintech Lending.

Pendahuluan

Pandemi yang terjadi belakangan ini telah mendesak pertumbuhan teknologi digital serta peningkatan penggunanya, salah satunya adalah peningkatan transaksi secara daring yang dilakukan lewat berbagai platform, misalnya *Financial Technology* (Fintech). *Financial Technology* (Fintech) diterapkan berdasarkan prinsip perlindungan konsumen serta manajemen risiko dan kehati-hatian dengan memperhatikan perluasan akses, kepentingan nasional, serta standar dan praktik internasional yang berlaku.

Fin ialah aktivitas pengalihan proses bisnis, model bisnis, dan instrumen keuangan yang menghasilkan nilai tambah baru di sektor jasa keuangan dengan membawa kemajuan digital saat ini yang dikenal dengan sebutan Inovasi Keuangan Digital (IKD).[1] Istilah *Fintech* merupakan singkatan dari *Financial Technology*. Fintech memiliki beberapa jenis, salah satu diantaranya adalah *peer-to-peer Landing* atau biasa disebut dengan pinjaman *online*.[2] *Peer-to-peer Landing* membagikan kemudahan dalam penggunaannya, dimana penerima serta pemberi dana bisa mendaftarkan dirinya kapanpun dan dimanapun hanya dengan memasukkan data individu ataupun data yang diperlukan para pengguna layanan pinjam meminjam serta beberapa verifikasi. Selain memberikan manfaat serta kemudahan, penyelenggara *peer-to-peer lending* juga memperoleh tantangan terhadap risiko *cyber security system* yang bisa memunculkan problematika yang merugikan masyarakat selaku pengguna layanan semacam penipuan, penyalahgunaan informasi, pencurian serta penjualan data pribadi, pemerasan, dan sebagainya. Lemahnya *cyber security system* dalam memproteksi data pribadi membuka kesempatan bagi peretas untuk mencuri data-data yang disimpan oleh penyelenggara semacam *fintech lending*, yang berakibat besar dan merugikan subjek data pribadi tersebut.

---

[1] Jadzil Baihaqi, '*Financial Technology Peer-To-Peer Lending* Berbasis Syariah di Indonesia', (2018), 1 Tawazun : *Journal Of Sharia Economic Law*.[119 – 120].

[2] 'Apa Itu Fintech Lending? Simak Pengertian Lengkapnya',(Investree.id, 2021) <https://blog.investree.id/marketplace-lending/apa-itu-fintech-lending-simak-pengertian-lengkapnya/#:~:text=fintech%20lending%20adalah%20singkatan%20dari,untuk%20mengembangkan%20modal%20melalui%20pendanaan> *accessed* 11 Maret 2022.

Banyaknya kasus ancaman *cyber* terjadi karena berbagai faktor, salah satunya yaitu tingginya akses pengguna online, termasuk pengguna layanan *fintech lending*. Banyaknya informasi data pribadi yang masuk dan lemahnya sistem keamanan pada teknologi online membuat serangan pencurian data pribadi menjadi mudah dilakukan.[3] Hal tersebut menjadi salah satu ancaman baru dalam perlindungan data pribadi seseorang, karena sering digunakan untuk mengancam dan memeras seseorang dengan memanfaatkan celah penggunaan kemajuan teknologi digital.

Berdasarkan publikasi *The Global Cybersecurity Index* (GCI) 2017 yang dirilis oleh *International Telecommunication Union* (ITU), kondisi *cyber security* di Indonesia masih tergolong dalam negara dengan kategori *cyber security* yang lemah dan dalam tahap peningkatan optimal *(maturing stage)*.[4] Untuk pertumbuhan ekonomi, pada dasarnya proteksi data pribadi yang bertabiat secara masif serta terstruktur akan berpotensi dalam penguatan ekonomi nasional serta investasi dalam perkembangan ekonomi secara global. Pemanfaatan informasi individu pada dasarnya tidak hanya sebatas dari perihal administratif saja, namun bisa mencakup banyak hal dalam aspek kehidupan bermasyarakat semacam hukum, politik, ataupun ekonomi.

Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah Pendekatan perundang-undangan *(Statute Approach)* dan Pendekatan Konseptual *(Conceptual Approach)*. Pendekatan *(Statute Approach)* digunakan untuk mengkaji terkait keberlakuan peraturan perundang-undangan dikaitkan dengan *fintech lending* terhadap ancaman *cyber security*. Sedangkan Pendekatan Konseptual *(Conceptual Approach)* digunakan untuk mengkaji landasan hukum utama pemberlakuan *fintech lending* serta perlindungan data pribadi bagi pengguna layanan *fintech lending* di Indonesia disesuaikan dan ditinjau dari pandangan-pandangan dan doktrin-doktrin yang dikembangkan dalam ilmu hukum.[5]

---

[3] S. Parulian *et al*., 'Ancaman dan Solusi Serangan Siber di Indonesia' (2021), 1 Jurnal Upi. [2].

[4] Damar A. S., A. J. Simon. R, 'Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia', (2019), 2 Jurnal Kajian Stratejik Ketahanan Nasional.[158].

[5] Peter Mahmud Marzuki, *Penelitian Hukum* (Kencana Prenada Media Group 2005).[177].

Bentuk Ancaman Cyber Security pada Layanan Fintech Lending di Indonesia

Bank Indonesia mendefinisikan *Financial Technology* sebagaimana diatur serta tertuang dalam Pasal 1 angka 1 Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial, yaitu teknologi finansial adalah penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru serta dapat berdampak pada stabilitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran.[6]

Fintech adalah bagian dari suatu *e-commerce* yang secara khusus berhubungan dengan transaksi keuangan yang memakai smartphone. Selain itu, *fintech* juga dapat dikatakan sebagai penggabungan layanan keuangan dengan teknologi informasi. *Fintech* tidak hanya termuat dalam area spesifik seperti pembiayaan ataupun model bisnis, namun juga memuat segala bisnis pada jasa keuangan dan simpan pinjam yang disediakan oleh kembaga keuangan.[7] Terdapat 2 (dua) grup pada jasa yang disediakan oleh perusahaan *fintech*, yaitu:[8]

1. Perusahaan *fintech* yang menyajikan jasa untuk perbankan.

   Misalnya menyediakan teknologi yang digunakan oleh bank untuk jasa keuangan.

2. Perusahaan *fintech* yang menyajikan jasa yang dilindungi oleh bank.

   Misalnya pembayaran.

Kini, terdapat lima bidang utama dalam *fintech,* yaitu:[9]

1. Keuangan dan investasi;
2. Operasi dan manajemen risiko;
3. Pembayaran dan infrastruktur;
4. Keamanan data dan monetisasi; dan
5. Antarmuka pelanggan.

Fintech Lending atau yang biasa disebut pinjaman *online* ini merupakan platform

---

[6] Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial

[7] Hyun – Sun Ryu, 'What Makes Users Willing or Hesitant to Use Fintech?: The Moderatoring Effect of User Type'. (2018). 118 Industrial Management & Data Systems.[541 – 569].

[8] Inna Romanova dan Marina Kudinska, *'Baking and Fintech: A Challenge or Opportunity?'*, (2016), 98 Contemporary Issue in Finance Current Challenges from Across Europe (Contemporary Studies In Economic and Finansial Analysis).[21 – 35].

[9] Douglas W. Arner, *et al*., 'The Evolution of Fintech: A New Post – Crisis Paradigm?', (2015), SSRN Electric Journal. <https://doi.org/10.2139/ssrn.2676553> *accessed* 2 Juni 2022.

online atau aplikasi yang menyediakan fasilitas kepada pemilik dana untuk dapat memberikan pinjaman kepada masyarakat secara langsung melalui teknologi digital. Peminjam juga dapat mengajukan permohonan pinjaman secara langsung melalui aplikasi tersebut dengan beberapa syarat dan ketentuan yang telah dicantumkan. Selanjutnya peminjam akan membayar pinjaman pokok tersebut dengan imbal hasilnya sesuai dengan kesepakatan.[10] Layanan *fintech lending* ini juga merupakan salah satu inovasi jasa keuangan dengan pemanfaatan teknologi yang memungkinkan pemberi pinjaman dan penerima pinjaman melakukan transaksi pinjam meminjam tanpa harus bertemu langsung.[11]

Banyaknya perusahaan *fintech lending* ini meningkatkan ketertarikan masyarakat Indonesia dengan banyaknya program yang ditawarkan, meskipun bunga *fintech lending* tersebut lebih tinggi apabila dibandingkan dengan bank. Selain itu, adanya masalah pada *fintech lending* ini diantaranya adanya penagihan dengan teror dan pengalihan kontak. Pemberi pinjaman pun dapat membaca semua jenis transaksi milik pengguna, membuktikan masih rendahnya perlindungan data pribadi

Cyber security adalah cara untuk menentukan pencapaian dan pemeliharaan sifat keamanan aset pengguna atas risiko keamanan yang signifikan dalam lingkungan *cyber*. Tujuan keamanan umum terdiri atas:[12]

1. Ketersediaan;

2. Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan; serta

3. Kerahasiaan.

Banyaknya *cyber crime* perlu adanya perhatian dan keseriusan dalam meningkatkan *cyber security* bagi suatu negara termasuk Indonesia. Menurut beberapa macam peristiwa pada beberapa tahun ke belakang, Indonesia adalah

---

[10] 'Marketplace Lending : Apa Itu Fintech Lending? Simak Pengertian Lengkapnya', (Investree.id, 2021) <https://blog.investree.id/marketplace-lending/apa-itu-fintech-lending-simak-pengertian-lengkapnya/> *accessed* 5 Maret 2022.

[11] Trisadini Prasastinah Usanti *et al*., *'Managing The Risk For Fintech Lending Amid The Global'*, (2021), 51 Jurnal Hukum & Pembangunan.[230].

[12] *Ibid.*

salah satu negara dengan *cyber security system* yang lemah. Salah satu kasus yang menyerang *cyber security system* yaitu peretasan data pada kartu kredit nasabah suatu bank akibat *hacker* yang berusaha menerobos ke dalam sistem pengamanan kartu nasabah bank. Hal tersebut terjadi pada pertengahan Mei 2014 yang membuat catatan lemahnya sistem *cyber security system* di Indonesia.[13]

Dalam hal ini Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, belum sepenuhnya memberikan perlindungan hukum kepada para pengguna layanan *fintech lending*. Banyaknya data yang terungkap di Indonesia membuat *cyber security* terkhusus perlindungan data pribadi di Indonesia perlu dipertanyakan. Data – data yang tersebar adalah data asli para pengguna yang dapat dimanfaatkan untuk tindakan kejahatan seperti telemarketing palsu. Tersebarnya data – data tersebut sangat merugikan pemiliknya dalam berbagai hal, seperti terganggunya privasi yang tertuang dalam Pasal 4 UU HAM dan dapat membahayakan keseharian pemilik data sebagaimana telah diatur dalam Pasal 9 UU HAM. Akan tetapi, hingga saat ini sering terjadi adanya kebocoran data pribadi melalui platform digital, terutama dalam aktivitas transaksi pada *financial technology (fintech) lending*.

Dalam fintech, terdapat 3 (tiga) bentuk ancaman *cyber security*, diantaranya:[14]

1. *Transaction Security*

Transaction security yaitu risiko keamanan yang mucul ketika melakukan proses transaksi.

2. ***Data Security***

---

[13] Ahmad Shofiyulloh, 'Cyber Security: Bagaimana Keamanan Dunia Siber di Indonesia?', (Kompasiana, 2021) <https://www.kompasiana.com/ahmadshofiyulloh0517/60e160a706310e58d9668932/cyber-security-bagaimana-keamanan-dunia-siber-di-indonesia> *accessed* 4 Juni 2022.

[14] Bisyron Wahyudi, 'Perlindungan Data Pribadi dan Ancaman Keamanan Siber di Fintech', (iForte, 2021) <https://iforte.id/news/detail/personal-data-protection-and-cyber-security-threats-in-fintech> *accessed* 5 Juni 2022.

Data security yaitu bentuk perlindungan terhadap data pribadi itu sendiri.

3. *Cyber Security*

Cyber security adalah risiko keamanan pada siber atau perlindungan terhadap serangan digital yang muncul.

Berkembangnya *fintech* menimbulkan risiko yang bermacam – macam tergantung karakteristik pada masing – masing fintech. Tantangan terbesarnya berupa risiko finansial dan risiko teknologi. Risiko teknologi yaitu berupa risiko *cyber security system* pada data pribadi akibat tindakan *cyber crime*. *Cyber crime* merupakan tindakan ilegal di bidang teknologi informasi dan komunikasi dengan meretas sistem komputer maupun jaringan internet untuk pencurian data, keuangan dan menyebarkan kode perangkat lunak berbahaya. Pelaku *cyber crime* biasanya memiliki tujuan untuk merusak jaringan organisasi dengan mencuri data pribadi, dokumen, hingga meretas rekening bank untuk mencuri uang.

Para pelaku *cyber crime* menggunakan celah pada fintech untuk melakukan pemerasan, penipuan, pencucian uang, bahkan kegiatan ilegal lainnya. Maka, perlu adanya peningkatan c*yber security* untuk melindungi data pribadi pengguna dari segala bentuk *cyber crime* dengan terus berinovasi dan mengembangkan teknologi yang ada.[15] Untuk menangani tindakan *cyber crime*, perlu adanya *cyber security*. Beberapa hal yang diperlukan dalam *cyber security*, yaitu: ketersediaan *(availability)*, kerahasiaan *(confidentiality)*, integritas *(integrity)*, otentikasi *(authentication)*, dan akuntabilitas *(acountability)*.[16]

Beragam serangan *pada cyber security* yang banyak dilakukan oleh pelaku *cyber crime* adalah *fintech attack*, yaitu:[17]

1. ***Trojan mobile banking***, merupakan penyerangan pada kode keamanan *mo-*

[15] M. Irfan, *et al*., '*Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions'*, (2018), 434 IOP Conferences Series: Materials Science and Engineering.[1 – 6].

[16] Pratham Singh dan R.S. Rajput, 'Cyber Security Analysis in the *Context of Digital Wallets'*, (2018), 4 International Journal of Advance Studies of Scientific Research.[522 – 525].

[17] Bruce Nikkel, '*Fintech Forensics: Criminal Investigation and Digital Evidence in Finansial Technologies'*, (2020), 33 *Forensic Science International: Investigasi Digital*. <Forensik fintech: Investigasi kriminal dan bukti digital dalam teknologi keuangan - ScienceDirect> *accessed* 5 Juni 2022.

bile banking yang dapat menyebar ke masyarakat luas;

2. ***Ransomeware***, merupakan tindakan memasukkan aplikasi jahat serta mengunci data pengguna guna memeras para pengguna dengan meminta uang tebusan;

3. ***Magecarting***, yaitu serangan pada *cyber security* yang mematok sistem transaksi pembayaran *online*.

Risiko lainnya terhadap ancaman *cyber security* semakin besar dengan meningkatnya teknologi serta kecepatan jaringan dari masa ke masa. *Hacking, phising* dan *malware* sangat memberikan pengaruh terhadap *cyber security compliance* pada sektor keuangan.[18] Pelaku *cyber crime* lebih tertarik untuk melakukan tindakan kejahatan *e-commerce* serta sistem pembayaran *online* karena mayoritas informasi pribadi serta data kartu kredit disimpan dan diproses melalui aplikasi tersebut. Oleh karena hal tersebut, penerapan *cyber security* yang handal harus dirancang dengan matang pada awal berdirinya suatu perusahaan fintech. Selanjutnya *cyber security* yang telah terpasang wajib dipasangkan dengan teknik deteksi serta investigasi yang handal pula guna melakukan pemulihan data apabila terjadi serangan *pada cyber security.*

Saat ini, perlu memperhatikan *cyber security* dalam menjalankan usaha fintech, karena adanya potensi kerugian yang sangat besarnya dari kejahatan digital ini. Selain itu, terdapat beberapa ancaman lain terhadap *cyber security system* pada fintech yang sering ditemukan, diantaranya:

1. ***Data Breaches*** **(Pelanggaran Data)**

Merupakan usaha pelaku dalam mengakses data – data termasuk data pribadi pengguna yang telah diamankan oleh perusahaan fintech yang mana akan disalahgunakan oleh pelaku seperti penjualan data, pemerasan, penggandaan kartu kredit, dan lain – lain.

2. **Penerapan** ***Security Protocol***

Merupakan tindakan yang dilakukan guna memastikan protokol keamanan yang tepat dan berkualitas terhadap keamanan bisnis fintech.

---

[18] Febrian Kwarto dan Madya Angsito, 'Pengaruh Cyber Crime Terhadap *Cyber Security Compliance* di Sektor Keuangan', (2018), 11 *Jurnal Akuntansi Bisnis*.[99 – 110]. <http://dx.doi.org/10.30813/jab.v11i2.1382> *accessed* 5 Juni 2022.

3. *Human Error*

Merupakan permasalahan keamanan yang timbul akibat kesalahan dari pengguna itu sendiri.

Pihak yang Bertanggung Gugat Terhadap Korban Tindakan Pencurian Data Pribadi pada Layanan *Fintech Lending* di Indonesia

Dalam menjalankan usahanya, penyelenggara layanan *fintech lending* di Indonesia memiliki tanggung jawab atas data – data yang diperoleh sepanjang berlangsungnya praktik usahanya. Hal ini diatur di dalam Pasal 44 Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi[19], yang mengatur mengenai kewajiban bagi penyelenggara.

Setiap penyelenggara layanan *fintech lending* juga wajib mendapatkan sertifikat dan menerapkan standar ISO/IIEC 27001 sesuai dengan standar yang ditentukan oleh Otoritas Jasa Keuangan dalam Surat Tanda Terdaftar. ISO/IEC 27001 adalah sertifikat berstandar internasional *Information Security Management System* (ISMS) yang menciptakan aturan atas tata kelola keamanan informasi guna menciptakan keyakinan dan jaminan pada klien serta mitra atas risiko maupun gangguan yang mungkin terjadi. Selain itu, setiap penyelenggara dapat memiliki standar keamanan informasi yang sama serta telah teruji.[20]

Pada generasi saat ini, kemajuan teknologi akan selalu berkaitan dengan berbagai kegiatan. Kegiatan masyarakat walaupun selalu berdampingan dengan adanya teknologi, banyak masyarakat yang tidak paham terkait teknologi. Perbuatan para pengguna layanan fintech lending yang tidak paham tentang *cyber security system* sangat mudah tertipu dan terjerumus kepada hal – hal yang dapat merugikan dirinya sendiri. Maka, sangat penting untuk pengguna dan penyelenggara layanan *fintech lending* dalam melakukan *pengembangan security awareness*, khususnya

[19] Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.

[20] PT Mitra Integrasi Informatika, 'Implementasi dan Sertifikasi ISO / IEC 27001: 2013 Bagi Industri Fintech #1', (mii.co.id, 2020) <https://www.mii.co.id/en/insight/ listing/2020/07/22/05/11/implementasi-dan-sertifikasi-iso-iec-27001-2013-bagi-industri-fintech-1> *accessed* 5 Juni 2022.

terhadap data pribadi. Penggunaan tanda tangan elektronik (TTE) yang terverifikasi merupakan salah satu cara untuk meminimalisir adanya penyalahgunaan data pribadi di berbagai kasus *cyber crime*, utamanya pada *fintech lending*.[21]

Berikut tindakan yang dapat dilakukan guna memberikan perlindungan pada layanan *fintech lending* atas serangan terhadap *cyber security*, diantaranya:[22]

1. Tindakan Inisiatif
2. Aturan Fintech
3. Langkah Khusus dalam Penerapan *Cyber Security* pada Layanan *Fintech Lending*

Cyber crime terkadang memanfaatkan adanya celah keamanan *cyber security* pada layanan *fintech lending*. Hal tersebut membuka pintu masuk terjadinya *cyber crime*. Untuk mengatasinya, diperlukan tindakan *cyber security* yang tepat, diantaranya:[23]

a. Memberikan perlindungan dan mengawasi titik akses nirkabel, titik akses jaringan, perangkat yang terhubung ke jaringan dengan sistem keamanan berlapis serta memonitori seluruh akses pengguna ke sumber informasi.
b. Memonitori dan memberikan batasan hak akses pengguna internal terhadap file maupun data yang hanya terhubung pada tugas / pekerjaan.
c. Mencegah dan mengamankan semua pengguna serta pengelola sistem yang menjadi target *cyber crime*.
d. Otentifikasi pada program pemindahan virus maupun *malware* serta serangan *cyber* lainnya.
e. Melakukan pemindaian secara berkala melalui program *anti-spyware* guna mendeteksi *spyware*, *adware* maupun *bot* (robot perangkat lunak) serta serangan *cyber* lainnya.
f. Pengadaan edukasi serta pelatihan terkait kesadaran bagaimana pentingnya keamanan dan kehati – hatian ketika menggunakan layanan internet, khususnya layanan *fintech lending*.

Dalam Pasal 1 angka 1 Peraturan Menteri Komunikasi dan Informatika RI Nomor

---

[21] Ananda Astri Dianka, 'Maraknya Pinjol Ilegal, Identitas Digital Bisa Jadi Solusi', (*TrenAsia.com,* 2021) <https://www.trenasia.com/marak-pinjol-ilegal-identitas-digital-bisa-jadi-solusi> *accessed* 2 Juni 2022.

[22] Alexander Anggono, 'Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review', (2021), 12 Jurnal Manajemen dan Organisasi (JMO.[246 – 247].

[23] M. Suganya Aravazhi, 'Understanding Cyber Crime and Cyber Laundering: Threat and Solution', (2020), 5 EPRA International Journal of Research and Development (IJRD).[34 – 38].

20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik[24], menyatakan bahwa :

> "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiaannya."

Konsep privasi yang melekat pada tiap manusia berkaitan erat dengan hak asasi manusia. Hal ini sebagaimana dinyatakan dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia (DUHAM) 1948 yang menyatakan bahwa hak privasi sebagai bagian dari hak asasi manusia yang harus dilindungi dan diakui, Pasal tersebut menyatakan:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to atteck upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack."*
> *"Tidak ada seorang pun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyuratnya, juga tidak diperkenakan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran itu."*

Menurut peraturan yang saja disahkan yaitu Undang – Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi[25], di dalam Pasal 1 angka 2 menyatakan bahwa:

> "Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi."

Pelindungan data pribadi merupakan salah satu bentuk dari perlindungan konsumen yang juga merupakan suatu upaya yang menjamin adanya kepastian hukum guna memberikan perlindungan kepada konsumen. Terdapat 5 (lima) asas perlindungan konsumen, yaitu asas manfaat, keadilan, keseimbangan, keamanan, dan keselamatan konsumen serta kepastian hukum.[26] Secara umum dikenal ada empat hak dasar konsumen, yaitu :

---

[24] Peraturan Menteri Komunikasi dan Informatika RI Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

[25] Undang – Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

[26] Bambang Sugeng Ariadi *et al*., 'Pola Penyelesaian Sengketa Konsumen Pada Transaksi Elektronik', (2021), V Lex Journal : Kajian Hukum & Keadilan.[122-123].

1. Hak untuk mendapatkan keamanan *(the right to safety);*
2. Hak untuk mendapatkan informasi *(the right to be informed);*
3. Hak untuk memilih *(the right to choose);*
4. Hak untuk didengar *(the right to be heard).*

Empat dasar tersebut diakui secara internasional. Dalam perkembangannya, beberapa organisasi konsumen yang tergabung dalam *The International Organization of Consumers Union* (IOCU) menambahkan lagi beberapa hak, seperti hak mendapatkan pendidikan konsumen, hak mendapatkan ganti kerugian, dan hak mendapatkan lingkungan hidup yang baik dan sehat.[27]

Perlindungan data pribadi adalah suatu hak *(privacy rights)* yang ada pada diri setiap orang dan harus dilindungi oleh negara sebagaimana ketentuan yang diatur di dalam Pasal 29 ayat (1) UU HAM[28]. Serta di dalam *privacy rights* setiap orang mempunyai hak untuk menjaga kerahasiaan diri sendiri. Selain itu, perlindungan data pribadi juga diatur di dalam Pasal 26 ayat (1) dan (2) Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berarti setiap orang berhak untuk menjaga kerahasiaan atas diri pribadinya. Apabila data pribadi tersebut bocor dan disalahgunakan oleh pihak lain yang tidak bertanggungjawab, maka pemilik data tersebut dapat mengajukan gugatan ke pengadilan. Gugatan yang diajukan berupa gugatan perdata yang diajukan sesuai dengan peraturan perundang – undangan yang ada. Ini artinya, kedua pasal tersebut sejatinya telah memberikan perlindungan atas data pribadi seseorang secara general.

Jadi, pada setiap kegiatan transaksi elektronik yang menggunakan informasi pribadi, para pengguna berkewajiban untuk melindungi data pribadi miliknya dengan berdasarkan pada aturan tersebut. Setiap informasi pribadi seseorang yang akan digunakan wajib meminta persetujuan pemilik data tersebut serta pihak yang bersangkutan wajib menjaga kerahasiaan data pribadi tersebut sebagaimana diatur dalam Pasal 5 UU Pelindungan Data Pribadi. Terkait dengan persetujuan pemrosesan data pribadi, telah diatur di dalam Pasal 22 UU Pelindungan Data Pribadi

[27] Shidarta, *Hukum Perlindungan Konsumen Indonesia* (Grasindo 2000).
[28] Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Kemudian, terkait perlindungan data pribadi pada layanan *fintech lending*, Otoritas Jasa Keuangan telah menerbitkan Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi. Pada Pasal 44 ayat (1) huruf a, telah diatur mengenai perlindungan data pribadi pengguna layanan *fintech lending*. Hal tersebut memiliki arti bahwa perusahaan *fintech lending* berkewajiban untuk melindungi data pribadi penggunanya dari proses dilakukannya perjanjian pinjam – meminjam sampai dengan berakhirnya suatu perjanjian. Kewajiban tersebut wajib dilaksanakan untuk menghindari adanya suatu peristiwa kebocoran data pribadi pengguna layanan *fintech lending*.

Kemudian, regulasi pada Pasal 44 ayat (1) huruf c Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 juga diartikan bahwa perusahaan *fintech lending* selaku penyelenggara maupun pemberi pinjaman tidak bisa menggunakan data pribadi pengguna untuk melakukan tindakan apapun apabila tidak ada persetujuan dari pengguna kecuali apabila ditentukan lain oleh peraturan perundang – undangan. Dengan adanya, regulasi tersebut, terdapat kepastian hukum atas perlindungan data pribadi. Perlindungan tersebut seperti hak perlindungan data pribadi yang diberikan kepada pengguna layanan *fintech lending*.

Jika terjadi pelanggaran atas hak yang dimiliki, maka pengguna layanan *fintech lending* dapat melakukan upaya hukum berupa upaya hukum non – yudisial dan upaya hukum yudisial. Upaya hukum non – yudisial yaitu upaya hukum yang dilakukan dengan mengajukan pengaduan kepada pengawas pada bidang jasa keuangan, dalam hal itu adalah Otoritas Jasa Keuangan. Setelah diajukannya aduan, maka Otoritas Jasa Keuangan akan memberikan teguran kepada perusahaan yang bersangkutan. Sedangkan, upaya hukum yudisial yaitu upaya hukum yang menembuk metode penegakan hukum. Upaya hukum yudisial ini diajukan selepas terjadinya suatu pelanggaran yang bertujuan untuk memperbaiki keadaan. Upaya hukum yudisial dilangsungkan dengan mengajukan gugatan ke pengadilan. Pengajuan gugatan tersebut tidak terbatas untuk menggugat perusahaan penyelenggara *fintech lending*, namun juga pihak pihak lain yang telah menyalahgunakan data pribadi milik pengguna meskipun tidak memilik hubungan hukum.

Sebagaimana ketentuan yang ada pada Bab XII UU Perlindungan Data Pribadi, dalam Pasal 64 menjelaskan bahwa dalam hal penyelesaian sengketa perlindungan data pribadi dapat juga dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya. Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses peradilan perlindungan data pribadi dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang – undangan yang ada, dan dalam hal diperlukannya untuk melindungi data pribadi, proses persidangan dalam kasus perlindungan data pribadi dilakukan secara tertutup.

Oleh karena itu, dengan adanya regulasi yang telah dijelaskan di atas, lahir suatu kepastian hukum berupa perlindungan hukum atas data pribadi para pengguna layanan *fintech lending*. Perlindungan hukum tersebut berupa perlindungan atas kerahasiaan data pribadi pengguna supaya data yang dimilikinya tidak disalahgunakan dan tetap terjaga kerahasiaannya oleh penyelenggara layanan *fintech lending*. Selain itu, pengguna layanan *fintech lending* dapat mengajukan upaya hukum jika data pribadinya disalahgunakan maupun disebarluaskan diluar persetujuannya.

Suatu tindakan yang melanggar hukum memberikan akibat hukum bagi pelaku, salah satunya pelanggaran terhadap data pribadi. Akibat hukum merupakan akibat dari suatu tindakan yang dilakukan guna memperoleh suatu akibat yang dikehendaki oleh pelaku dan yang diatur oleh hukum.[29] Tindakan tersebut disebut tindakan hukum. Singkatnya, akibat hukum merupakan akibat dari suatu tindakan hukum. Maka, akibat hukum dari suatu tindakan pelanggaran data pribadi oleh penyelenggara layanan *fintech lending* adalah penjatuhan sanksi.

Dalam ketentuan hukum perdata, salah satu jenis perikatan berdasarkan sumbernya yaitu perikatan yang lahir dari perjanjian sebagaimana diatur di dalam Pasal 1233 BW.[30] Adanya peristiwa pinjam – meminjam uang termasuk jenis perikatan yang lahir dari suatu perjanjian.

---

[29] R. Soeroso, *Pengantar Ilmu Hukum* (Sinar Grafika 2011).[295].

[30] Zaeni Asyhadie, *Hukum Bisnis dan Pelaksanaannya di Indonesia* (Raja Grafindo Persada 2006).[24].

Ketika melakukan suatu perjanjian, wajib memenuhi syarat sahnya suatu perjanjian sebagaimana diatur dalam Pasal 1320 BW[31]. Di dalam suatu kontrak perjanjian, perlu memuat suatu hak dan kewajiban masing – masing pihak untuk mendapatkan suatu perlindungan hukum bagi para pihak. Namun dalam pelaksanaannya, pihak penyelenggara layanan *fintech lending* tidak melaksanakan kewajibannya yang mengakibatkan kerugian bagi pengguna layanan *fintech lending*.[32] Pihak yang dirugikan secara yuridis formal dapat mengajukan gugatan ganti kerugian sebagaimana diatur dalam Pasal 1365 BW.

Apabila dikaitkan dengan adanya kebocoran data pribadi pengguna yang diakibatkan oleh penyelenggara layanan *fintech lending*, maka hal tersebut dapat diklasifikasikan sebagai pencemaran nama baik. Hal tersebut telah diatur di dalam Pasal 27 ayat (3) Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Oleh karenanya, sanksi yang dapat diberikan apabila mengacu pada Pasal 45 Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, kasus pelanggaran data pribadi pada suatu perusahaan layanan *fintech lending* dapat dikenakan sanksi administratif, sebagaimana diatur di dalam Pasal 49 ayat (1) Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022.

Kemudian, pada Pasal 49 ayat (2) dan (3) Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tersebut menyatakan bahwa sanksi administratif dapat disertai dengan pemblokiran sistem elektronik milik penyelenggara. Sedangkan sanksi administratif berupa denda dapat dikenakan secara tersendiri atau secara bersama – sama dengan pengenaan sanksi administratif berupa peringatan tertulis, pembatasan kegiatan usaha dan pencabutan izin.

Sanksi administratif tersebut dilayangkan oleh Otoritas Jasa Keuangan selaku pengawas kegiatan pada bidang jasa keuangan, diantaranya pada layanan *fintech lending*. Sanksi tersebut dijatuhkan kepada penyelenggara layanan *fintech lending* setelah Otoritas Jasa Keuangan menerima laporan terkait pelanggaran yang

[31] Staatsblad 1847 Nomor 23 tentang *Burgerlijk Wetboek Voor Indonesia (Burgerlijk Wetboek)*
[32] I Ketut Oka Setiawan, *Hukum Perikatan*, Cet. III (Sinar Grafika 2018).[19].

dilakukan dari beberapa pihak yang dirugikan. Namun, sebelum dijatuhkannya sanksi tersebut, perlu adanya pemeriksaan dan sanksi akan dilayangkan jika terbukti adanya pelanggaran yang dilakukan oleh penyelenggaran terhadap peraturan perundang – undangan dan merugikan beberapa pihak.

Sehingga apabila dari perusahaan mengalami kegagalan dalam hal pengendalian data pribadi penggunanya, maka perusahaan sebagai pengendali data pribadi penggunanya wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada pengguna yang bersangkutan dan lembaga sebagaimana ketentuan pada Pasal 46 UU Pelindungan Data Pribadi. Pemberitahuan tersebut minimal memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, serta upaya yang telah dilakukan oleh perusahaan dalam menangani dan memulihkan data pibadi tersebut. Apabila diperlukan, perusahaan juga wajib memberitahukan kepada masyarakat mengenai kegagalannya dalam melindungi data pribadi penggunanya.

Mengenai pencurian data pribadi, pembuatan data pribadi palsu, maupun memalsukan data pribadi dapat juga dikenakan sanksi pidana dengan merujuk pada ketentuan pada Pasal 66 – 68 UU Pelindungan Data Pribadi. Selain dijatuhi pidana, pelaku juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian sebagaimana ketentuan pada Pasal 69 UU Perlindungan Data Pribadi. Terkait sanksi administratif, pada UU Pelindungan Data Pribadi, diatur di dalam Pasal 57 mengenai jenis pelanggaran, jenis sanksi, serta tata cara pengenaan sanksi.

Perkembangan informasi terus berjalan mengikuti kemajuan teknologi. Perkembangan informasi tersebut melahirkan permasalahan baru terhadap *track record* data pribadi setiap orang dalam penggunaan teknologi informasi setiap waktu. Umumnya masyarakat menggunakan platform digital yang memerlukan beberapa data serta identitas pengguna guna keberlangsungan penggunaan layanan tersebut. Hal tersebut membuat para pengguna harus mengawasi serta menjaga penggunaan layanan digital tersebut supaya dapat dipertanggungjawabkan. Namun, terkadang beberapa data serta identitas para pengguna tersebut dapat disalahgunakan

oleh beberapa pihak.[33] Maka, perlu diterapkannya suatu regulasi yang dirasa bisa memberikan batasan dalam penggunaan layanan digital guna melindungi data pribadi para pengguna serta tidak terjadi adanya penyalahgunaan data pribadi para pengguna layanan digital.[34]

Istilah lain atas berlakunya aturan tentang yurisdiksi teknologi digital yaitu *Lex Digitalis*. *Lex Digitalis* merupakan suatu aturan yang berperan sebagai implementasi dari konsep legalitas atas pemanfaatan teknologi digital, sehingga tidak ada perbuatan hukum pada ruang digital yang tidak dapat dijangkau oleh yurisdiksi normatif. Pada dunia siber, yurisdiksi harus mempunyai konektivitas tanpa batas.[35]

Adapun berdasarkan Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara, Direktorat Operasi Keamanan Siber, Deputi II, memiliki tugas untuk mengkoordinasikan perumusan dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber. Dalam pelaksanaannya, Direktorat Operasi Keamanan Siber mengelola tim tanggap insiden siber nasional yang menerima layanan aduan siber melalui pusat kontak siber. Adapun prosedur pengaduan siber, diantaranya:[36]

1. Penerimaan aduan insiden siber melalui telepon 02178833610 atau surel bantuan70@bssn.go.id;
2. Pencatatan aduan insiden siber baik identitas pelapor disetai dengan data pendukung serta bukti terjadinya insiden siber;
3. Notifikasi penerimaan aduan insiden siber;
4. Verifikasi aduan insiden siber;
5. Observasi dan investigasi aduan insiden siber;

---

[33] Mark de Reuver, et al., 'The Digital Platform: A Research Agenda', (2018), Journal of Information and Technology. <The Digital Platform: A Research Agenda (sagepub.com)> *accessed* 8 Juni 2022.

[34] Yusuf, 'Perlindungan Data Pribadi: Tak Cukup Sanksi, Butuh Kesadaran!', (Kementerian Komunikasi dan Informasi Republik Indonesia, 2020) <Kementerian Komunikasi dan Informatika (kominfo.go.id)> *accessed* 8 Juni 2022.

[35] Farhan Abel Septian Rachmadani dan Sinta Dewi Rosadi, "Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada *Smart Contract* Ditinjau dari Hukum Positif di Indonesia*",* (2021), 5 Jurnal Sains Sosio Humaniora. <View of Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia (unja.ac.id)> *accessed* 8 Juni 2022.

[36] Badan Siber dan Sandi Negara, "Aduan Siber", (bssn.go.id, 2021) <https://bssn.go.id/aduan-siber/> *accessed* 18 Desember 2022.

6. Pemberian rekomendasi cara penanggulangan insiden siber;
7. Jika adinistrator IT/pemilik aset tidak dapat menyelesaikan insiden siber dapat meminta BSSN untuk dapat membantu menindaklanjuti aduan insiden siber tersebut.

Sehingga, apabila mengalami insiden siber, pelapor diminta untuk mengumpulkan bukti insiden tersebut berupa foto/*screenshot* (tangkapan layar), kemudian dikirimkan disertai dengan pembuatan laporan ke pusat kontak siber BSSN dengan menghubungi nomor telepon (021) 78833610 atau *email* bantuan70@bssn.go.id untuk meminta bantuan penanganan insiden siber dari BSSN. BSSN juga telah mengeluarkan maklumat untuk sanggup secara profesional dan bertanggung jawab dalam melayani aduan siber secara berkelanjutan dengan peraturan yang berlaku.[37]

Perlindungan terhadap pencurian data pribadi pada teknologi digital juga diatur dalam undang – undang serta peraturan pemerintah, diantaranya:

1. Pasal 40 dan Pasal 42 ayat (1) Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi[38]
2. Pasal 26 ayat (1), Pasal 30 ayat (3), dan Pasal 32 Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[39];
3. Pasal 40 Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang – Undang Nomor 7 Tahun 1992 tentang Perbankan[40]
4. Pasal 44 huruf (h) Undang – Undang Nomor 43 Tahun 2009 tentang Kearsipan[41];
5. Pasal 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.[42]

Selain adanya aturan yang mengatur tentang perlindungan data khususnya yang ada kaitannya dengan platform digital, terdapat beberapa aturan terkait upaya hukum yang dapat ditempuh oleh korban pencurian data pribadi pada platform digital. Utamanya yaitu aturan terkait permohonan ganti kerugian atas pelanggaran data

[37] *Ibid.*
[38] Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
[39] Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[40] Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang – Undang Nomor 7 Tahun 1992 tentang Perbankan.
[41] Undang – Undang Nomor 43 Tahun 2009 tentang Kearsipan.
[42] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

pribadi sebagaimana diatur di dalam Pasal 1365 BW yang kemudian dijelaskan lebih lanjut pada Pasal 1366 BW.

Jika pertanggungjawaban atas pelanggaran data pribadi diterapkan pada platform digital khususnya pada layanan *fintech lending*, hal tersebut dapat mengacu pada Pasal 1 ayat (3) Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen[43]. Oleh sebab itu, perusahaan *fintech lending* pun wajib bertanggung jawab atas kerugian konsumennya sebab perusahaan *fintech lending* diklasifikasikan sebagai pelaku usaha. Salah satu upaya yang wajib dilakukan oleh pelaku usaha diatur di dalam Pasal 19 ayat (1) Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Pencurian data pribadi dalam platform digital termasuk pada unsur tersebut karena perusahaan *fintech lending* seharusnya bertanggung jawab atas data pribadi konsumennya karena para konsumen tersebut menggunakan jasa yang ditawarkan oleh perusahaan *fintech lending*. Hal tersebut ditawarkan guna mendapatkan keuntungan serta dapat dijadikan dasar mengapa perusahaan *fintech lending* harus bertanggung jawab jika terjadi kebocoran data pribadi penggunanya sebagaimana ketentuan pada Pasal 45 ayat (1) Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lalu, diperjelas terkait tata cara mengajukan gugatan terhadap pelaku usaha di dalam Pasal 32 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Apabila melihat dari Rancangan Undang – Undang Perlindungan Data Pribadi yang saat ini telah disahkan menjadi Undang – Undang Perlindungan Data Pribadi, dapat merujuk pada Bab XIII tentang Larangan dalam Penggunaan Data Pribadi. Terkait pencurian data pribadi, dapat merujuk pada Pasal 65 ayat (1), bahwa:

> "Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi."

[43] Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Selain itu, di dalam Pasal 66 juga dijelaskan bahwa:

> "Setiap orang dilarang membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain."

Negara juga berkewajiban dalam mengambil tindakan guna merealisasikan hak warga negaranya untuk dapat berkomunikasi memperoleh informasi yang merupakan salah satu aspek penting dalam inovasi yang dilakukan dalam transformasi digital negara Indonesia. Hal tersebut telah diamanatkan dalam Pasal 28F Undang – Undang Dasar Negara Republik Indonesia Tahun 1945.[44] Secara spesifiknya, di dalam Pasal 1 angka 1 Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Pada proses perkembangannya, sektor telekomunikasi memiliki peran penting di beberapa aspek di Indonesia. Dalam berkembangnya penggunaan teknologi informasi, menghadapi adanya perubahan besar dan hal tersebut berdampak pada perlindungan data pribadi, diantaranya dalam implementasi *e-commerce* pada sektor pendidikan, kesehatan, perdagangan, pemerintahan, serta telekomunikasi. Tindakan yang dilakukan masyarakat dalam memanfaatkan teknologi informasi didorong dengan adanya ketersediaan keutuhan *(integrity)* serta kerahasiaan *(confidentiality)* terkait informasi pada ruang siber.[45]

Pemerintah kemudian menerbitkan Peraturan Pemerintah Nomor 46 Tahun 2021 tentang Pos[46], Telekomunikasi, dan Penyiaran (Postelsiar) pasca diterbitkannya Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja [47]sebagai aturan lanjutan dari Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja. Dengan adanya Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, seluruh pelaku usaha utamanya per usahaan fintech dapat mendaftarkan diri serta tunduk pada hukum positif Indonesia.

Kesimpulan

Terdapat 3 (tiga) bentuk ancaman *cyber security* dalam fintech, diantaranya *transaction security*, *data security,* dan *cyber security*. Tantangan terbesar pada

[44] Undang – Undang Dasar Negara Republik Indonesia Tahun 1945.

[45] Muhammad Hasan Rumlus dan Hanif Hartadi, 'Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik', (2020) 11 Jurnal HAM.

[46] Peraturan Pemerintah Nomor 46 Tahun 2021 tentang Pos.

[47] Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja

fintech berupa risiko finansial dan risiko teknologi yang berupa risiko *cyber security* pada data pribadi akibat tindakan *cyber crime*. Selain itu, terdapat beragam serangan *pada cyber security* yang banyak dilakukan oleh pelaku *cyber crime* yaitu *fintech attack*, yang diantaranya *trojan mobile banking*, *ransomeware*, dan *magecarting*. *Hacking, phising* dan *malware* juga merupakan ancaman yang sangat memberikan pengaruh terhadap *cyber security compliance* pada sektor keuangan. Pelaku *cyber crime* lebih tertarik untuk melakukan tindakan kejahatan *e-commerce* serta sistem pembayaran *online* karena mayoritas informasi pribadi serta data kartu kredit disimpan dan diproses melalui aplikasi tersebut. Kemudian, terdapat beberapa ancaman lain terhadap *cyber security* pada fintech yang sering ditemukan, diantaranya *data breaches* (pelanggaran data), penerapan *security protocol*, dan *human error*.

Setiap penyelenggara layanan *fintech lending* juga diwajibkan mendapatkan sertifikat dan menerapkan standar ISO/IIEC 27001 sesuai dengan standar yang ditentukan oleh Otoritas Jasa Keuangan dalam Surat Tanda Terdaftar. Dengan adanya regulasi pada Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 serta UU Perlindungan Data Pribadi, maka terdapat kepastian hukum atas perlindungan data pribadi. Dalam hal kebocoran maupun pencurian data, maka pengguna layanan *fintech lending* dapat melakukan upaya hukum berupa upaya hukum non – yudisial dan upaya hukum yudisial. Selain itu, juga dapat membuat aduan kepada Badan Siber dan Sandi Negara dengan mengumpulkan bukti insiden tersebut berupa foto/*screenshot* (tangkapan layar), yang kemudian dikirimkan disertai dengan pembuatan laporan ke pusat kontak siber BSSN dengan menghubungi nomor telepon (021) 78833610 atau *email* bantuan70@bssn.go.id untuk meminta bantuan penanganan insiden siber. BSSN juga telah mengeluarkan maklumat untuk sanggup secara profesional dan bertanggung jawab dalam melayani aduan siber secara berkelanjutan dengan peraturan yang berlaku.

Daftar Bacaan

Buku

Asyhadie, Zaeni, *Hukum Bisnis dan Pelaksanaannya di Indonesia*, (Citra Aditya, 2006).

Ketut Oka Setiawan, I, *Hukum Perikatan* (Sinar Grafika 2018).

Marzuki, Peter Mahmud, *Penelitian Hukum* (Kencana Prenada Media Group 2008).

Soeroso, R, *Pengantar Ilmu Hukum* (Sinar Grafika 2011).

Jurnal

Abel Septian R, Farhan dan Dewi Rosadi, Sinta, 'Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau dari Hukum Positif di Indonesia', (2021), 5 Jurnal Sains Sosio Humaniora. <View of Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia (unja.ac.id)> *accessed* 8 June 2022.

Anggono, Alexander, *'Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review'*, (2021), 12 Jurnal Manajemen dan Organisasi (JMO).

Ariadi, Bambang S., *et al*., 'Pola Penyelesaian Sengketa Konsumen Pada Transaksi Elektronik', (2021), 2 Lex Journal : Kajian Hukum & Keadilan.

Arner, W., *et al*., 'The Evolution of Fintech: A New Post-Crisis Pradigm', (2015), Geo. J. Int.

Baihaqi, Jadzil, *'Financial Technology Peer-To-Peer Lending* Berbasis Syariah di Indonesia', (2018) 1 Journal of Sharia Economic Law.

De Reuver, Mark, et al., 'The Digital Platform: A Research Agenda', (2018) Journal of Information and Technology. <The Digital Platform: A Research Agenda (sagepub.com)> *accessed* 8 June 2022.

Irfan, M et al., 'Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions', (2018), 434 IOP Conferences Series:Materials Science and Engineering.

Kwarto, Febrian dan Angsito, Madya, 'Pengaruh Cyber Crime Terhadap Cyber Security Compliance di Sektor Keuangan', (2018) 11 Jurnal Akuntansi Bisnis. <http://dx.doi.org/10.30813/jab.vlli2.1382> *accessed* 5 June 2022.

Nikkel, Bruce, 'Fintech Forensics: Criminal Investigation and Digital Evidence in Finansial Technologies', (2020), 33 Forensic Science International: Investigasi Digital. <Forensik fintech: Investigasi kriminal dan bukti digital dalam teknologi keuangan - ScienceDirect> *accessed* 5 June 2022.

Parulian, Sahat *et al*, 'Ancaman dan Solusi Serangan Siber di Indonesia' (2021), 1 Jurnal UPI.

Romanova, I. dan Kudinska, M., 'Banking and Fintech: A Challenge or Opportunity?', (2016), 98 Contemporary Issue in Finance: Current Challenges from Across Europe (Contemporary Studies in Economic and Finansial Analysis).

Ryu, H.S., 'What Makes Users Willing or Hesitant to Use Fintech?: The

Suganya Araazhi, M, 'Understanding Cyber Crime and Cyber Laundering: Threat and Solution', (2020), 5 EPRA International Journal of Research and Development (IJRD).

Usanti, Trisadini Prasastinah *et al*, 'Managing The Risk For Fintech Lending Amid The Global', (2021), 51 Jurnal Hukum & Pembangunan.

Peraturan Perundang-Undangan

Undang – Undang Dasar Negara Republik Indonesia Tahun 1945.

Staatsblad 1847 Nomor 23 tentang *Burgerlijk Wetboek Voor Indonesia (Burgerlijk Wetboek).*

Undang–Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 3472).

Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang - Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790).

Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Lembaga Negara Republik Indonesia Tahun 1999 Nomor 22, Tambahan Lembaga Negara Republik Indonesia Nomor 3821).

Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881).

Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165, Tambahan Lembaran Negara Republik Indonesia Nomor 3886).

Undang – Undang Nomor 32 Tahun 2002 tentang Penyiaran (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 139, Tambahan Lembaran Negara Republik Indonesia Nomor 4252).

Undang – Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran Negara Republik Indonesia Nomor 4674).

Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58,Tambahan Lembaga Negara Republik Indonesia Nomor 4843).

Undang – Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846).

Undang – Undang Nomor 38 Tahun 2009 tentang Pos (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 146, Tambahan Lembaran Negara Republik Indonesia Nomor 5065).

Undang – Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071).

Undang – Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253).

Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang–Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573).

Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 46 Tahun 2021 tentang Pos, Telekomunikasi, dan Penyiaran

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial.

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi informasi.

Deklarasi Universal Hak Asasi Manusia (DUHAM), 1948.

Internet

'Apa Itu Fintech Lending? Simak Pengertian Lengkapnya', (Investree.id,2021) <https://blog.investree.id/marketplace-lending/apa-itu-fintech-lending-simak-pengertian-lengkapnya/#:~:text=fintech%20lending%20adalah%20singkatan%20dari,untuk%20mengembangkan%20modal%20melalui%20pendanaan>*accessed* 11 Maret 2022.

Astri Dianka, Ananda, 'Maraknya Pinjol Ilegal, Identitas Digital Bisa Jadi Solusi', (TrenAsia.com, 2021) <https://www.trenasia.com/marak-pinjol- ilegal-identitas-digital-bisa-jadi-solusi> *accessed* 2 Juni 2022.

Badan Siber dan Sandi Negara, 'Aduan Siber', (bssn.go.id, 2021) <https://bssn.go.id/aduan-siber/> *accessed* 18 Desember 2022.

'Marketplace Lending : Apa Itu Fintech Lending? Simak PengertianLengkapnya', (Investree.id, 2021) <https://blog.investree.id/marketplace-lending/apa-itufintech-lending-simak-pengertian-lengkapnya/> *accessed* 5 Maret 2022.

Wahyudi, Bisyron, 'Perlindungan Data Pribadi dan Anca,an Keamanan Siber di Fintech', (iForte, 2021) <https://iforte.id/news/detail/personal-data-protection-and-cyber-security-threats-in-fintech> *accessed* 5 Juni 2022.

PT Mitra Integrasi Informatika, 'Implementasi dan Sertifikasi ISO / IEC 27001: 2013 Bagi Industri Fintech #1, (mii.co.id, 2020) <https://www.mii.co.id/en/insight/ listing/2020/07/22/05/11/implementa si-dan-sertifikasi-iso-iec-27001-2013-bagi-industri-fintech-1> *accessed* 5 Juni 2022.

Shofiyulloh, Ahmad, 'Cyber Security: Bagaimana Keamanan Dunia Siber di Indonesia?', (Kompasiana, 2021) <https://www.kompasiana.com/ahmad shofiyulloh0517/60e160a706310e58d9668932/cyber-security-bagaimana-keamanan-dunia-siber-di-indonesia> *accessed* 4 Juni 2022.

--halaman ini sengaja dibiarkan kosong--