



## Landasan Konstitusional Perlindungan Data Pribadi Pada Transaksi Fintech Lending di Indonesia

Afif Noor<sup>1</sup>, Dwi Wulandari<sup>2</sup>

<sup>1</sup>Fakultas Syari'ah dan Hukum Universitas Islam Negeri Walisongo Semarang

<sup>2</sup>Fakultas Ilmu Budaya Universitas Diponegoro Semarang

Email: [afifwali9@gmail.com](mailto:afifwali9@gmail.com)

**Abstract:** Financial Technology (fintech) lending, better known as peer-to-peer lending (P2PL), is a fast-growing fintech. In carrying out its business activities, the fintech lending platform always asks for personal data of prospective borrowers (borrowers), often misused, even though personal data is a person's privacy and human rights. This study aims to find a constitutional basis for protecting personal data, both formal and material. This research is a normative juridical study using a statutory approach. The data source comes from secondary data in the form of primary legal materials and secondary legal materials. The data obtained were analyzed descriptively using a deductive mindset. Based on the research, it was found that the constitutional basis of fintech lending was explicitly stipulated in Article 28 of the 1945 Constitution. Thus, the existence of such personal data must be protected by law. This form of regulation has solid binding power. It can impose sanctions that are detrimental to lawbreakers considering the existing laws related to fintech lending transactions such as POJK No.77/2016 have not been able to guarantee the security of personal consumer data. Policymakers need to carry out legal reforms by forming a personal data protection law that protects parties in fintech lending transactions in particular or information technology-based transactions in general.

**Keywords:** Constitutional foundation; Protection of Personal Data; Fintech Lending

**Abstrak:** Financial Technology (fintech) lending atau yang lebih dikenal dengan peer to peer lending (P2PL) merupakan salah satu fintech yang tumbuh dengan pesat. Dalam menjalankan kegiatan usahanya platform fintech lending selalu meminta data pribadi calon peminjam (borrower) yang seringkali disalahgunakan, padahal data pribadi merupakan privasi dan hak asasi seseorang. Penelitian ini bertujuan untuk menemukan landasan konstitusional perlindungan data pribadi baik formil maupun materiil. Penelitian ini merupakan penelitian yuridis normatif dengan menggunakan pendekatan undang-undang. Sumber data berasal dari data sekunder berupa bahan hukum primer dan bahan hukum sekunder. Data yang diperoleh dilakukan analisis deskriptif dengan menggunakan pola pikir deduktif. Berdasarkan penelitian ditemukan bahwa landasan konstitusional fintech lending secara khusus tertuang dalam Pasal 28 UUD 1945. Dengan demikian, keberadaan data pribadi tersebut harus dilindungi oleh hukum dalam bentuk undang-undang agar mempunyai daya ikat yang kuat dan dapat memberikan sanksi yang menjerakan bagi para pelanggar hukum mengingat perundang-undangan yang terkait dengan transaksi fintech lending yang telah ada seperti POJK No.77/2016 belum mampu memberikan jaminan perlindungan terhadap keamanan data pribadi konsumen. Pengambil kebijakan perlu melakukan pembaharuan hukum melalui pembentukan undang-undang perlindungan data pribadi yang melindungi para pihak dalam transaksi fintech lending khususnya atau transaksi berbasis teknologi informasi pada umumnya.

**Kata Kunci:** Landasan Konstitusional; Perlindungan Data Pribadi, Fintech Lending

## A. Pendahuluan

Transaksi *fintech (financial Technology)lending* atau biasa disebut dengan *peer to peer lending (P2PL)* di Indonesia mengalami pertumbuhan yang luar biasa seiring dengan semakin tingginya penggunaan teknologi informasi sebagai penunjang kehidupan manusia. Berdasarkan data Otoritas Jasa Keuangan (OJK) per 31 Desember 2020, akumulasi penyaluran pinjaman nasional mencapai Rp. 155,90 triliun naik 91,30% *year on year (yoy)* dibanding Desember 2019 yang hanya sebesar Rp. 81.49 triliun. Akumulasi penyaluran dana pinjaman pada Desember 2020 ini, jauh lebih tinggi jika dibandingkan dengan akumulasi penyaluran dana pada Desember 2018 yang hanya mencapai Rp. 22.67 triliun. Peningkatan jumlah penyaluran pinjaman tersebut sejalan dengan peningkatan jumlah rekening pemberi pinjaman (*lender*) dan penerima pinjaman (*borrower*). Secara rinci sampai dengan Desember 2020 akumulasi jumlah rekening *lender* mencapai 716.963 entitas, naik 18,32% *yoy* dibanding Desember 2019 yang berjumlah 605.935 entitas. Jumlah rekening *borrower* mengalami pertumbuhan yang jauh lebih tinggi dibanding dengan pertumbuhan jumlah rekening *lender*. Hingga Desember 2020, jumlah rekening peminjam telah mencapai 43.561.362 entitas dan 16.354.541 entitas aktif, meningkat 134,59% dari tahun ke tahun dari 18.569.123 entitas pada Desember 2019<sup>1</sup>. Tingginya pertumbuhan *fintech lending* antara lain disebabkan oleh kebutuhan masyarakat dalam mencari pendanaan dalam rangka menunjang kegiatan usaha maupun konsumsi masyarakat<sup>2</sup>.

Dalam memberikan pinjaman, penyelenggara jasa layanan pinjam meminjam uang secara elektronik atau *platform fintech lending* melakukan analisa melalui apa yang disebut dengan *scoring system* atau *credit scoring*<sup>3</sup> dan *artificial intelligence (AI)*. Kedua hal ini merupakan andalan *platform P2PL* dalam memberikan pinjaman. Semua analisis kredit dilakukan dengan mengandalkan dukungan data (*big data*) milik *platform fintech lending* yang diperoleh dari beberapa pihak dengan dukungan data pribadi yang diserahkan oleh *borrower*. Pada saat mengajukan pinjaman, *borrower* diharuskan meng-*upload* foto copy Kartu Tanda Penduduk dan dapat mengakses *phonebook*, kontak, kamera, mikrofon dan lokasi dan dapat mengakses IMEI (*International Mobile Equipment Identity*) telepon. Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) juga ingin mengakses ke *device, call log, short message service*<sup>4</sup>. Keleluasaan *platform fintech lending* untuk mengakses data pribadi ini berakibat banyaknya aduan yang terkait dengan perilaku *platform fintech lending* dalam menjalankan kegiatan usahanya terutama dalam hal melakukan penagihan atas kewajiban *borrower* untuk melakukan pembayaran pinjamannya.

---

<sup>1</sup>Otoritas Jasa Keuangan RI, (2020) *Data Statistik*, Available online from <https://www.ojk.go.id/id/kanal/iknb/data-danstatistik/fintech/Documents/Statistik%20Fintech%20Lending%20Desember%202020.pdf>, OJK.go.id [Accessed Feb 02, 2021].

<sup>2</sup>Hasil Studi *Institute For Development of Economics and Finance (Indef)* dan Asosiasi Fintech Indonesia, 2019, *Studi Dampak Fintech P2P Lending terhadap Perekonomian Nasional*, dapat diakses di <https://indef.or.id/source/research/Studi%20Dampak%20Fintech%20P2P%20Lending%20terhadap%20Perekonomian%20Nasional.pdf> diakses tanggal 10 april 2021

<sup>3</sup>Proses *credit scoring* merupakan proses yang harus dilakukan *marketplace P2PL* untuk menentukan layak atau tidaknya konsumen untuk dipinjam uang setidaknya berdasarkan 15 variabel yang telah ditentukan.

<sup>4</sup> Yanurisa Ananta, (2019), *Akses Data Dibatasi & Kredit Macet Fintech Tembus 3,18%*, Available online from <https://www.cnbcindonesia.com/tech/20190401174515-37-64144/akses-data-dibatasi-kredit-macet-fintech-tembus-318>, CNBC Indonesia, [Accessed Feb 02, 2021].

Berdasarkan catatan AFPI sepanjang Januari – November 2020 telah menerima 3.726 laporan pengaduan konsumen *Fintech Peer to Peer* (P2P), 46 % dari laporan pengaduan tersebut merupakan aduan mengenai penagihan tidak beretika dan 7,7 % pengaduan pelanggaran data pribadi<sup>5</sup>. Sedangkan akhir Juni 2019 aduan terhadap P2PL mencapai 4.500 aduan<sup>6</sup>. Hal ini menunjukkan adanya penyimpangan perilaku dari *platform* P2PL dalam menggunakan data pribadi nasabah atau konsumennya. Meskipun tahun 2020 mengalami penurunan akan tetapi pelanggaran data pribadi masih menjadi persoalan yang harus diperhatikan mengingat data pribadi seringkali disalahgunakan pada transaksi bisnis yang terkait dengan penggunaan teknologi informasi sebagaimana temuan *International Computer Science Institute* (ICSI) yang menemukan bahwa data pengguna telah dikumpulkan secara paksa oleh 1.325 aplikasi Android. ICSI melakukan pengamatan terhadap 88.000 lebih aplikasi pada *Google Play Store* dan melakukan pelacakan terhadap transfer data dari aplikasi saat pengguna menolak izin yang diminta<sup>7</sup>.

Hal tersebut menunjukkan pelaku usaha berbasis teknologi informasi mempunyai peluang yang besar untuk melakukan pelanggaran terhadap perlindungan data pribadi. Menurut kajian Safenet, pencurian maupun penyalahgunaan data pribadi dilatarbelakangi oleh tiga motif. *Pertama*, motif ekonomi, pelanggaran ini dilakukan melalui jual beli data secara ilegal. *Kedua* motif politik, pelanggaran jenis ini dilakukan dengan cara memanfaatkan data yang diperoleh secara ilegal dalam rangka memperoleh kekuasaan, seperti membuka data pribadi lawan politik secara terbuka. *Ketiga*, motif ancaman, yang dilakukan dalam rangka untuk memberikan ancaman pada orang lain agar merasa takut<sup>8</sup>.

Dalam industri *fintechlending* munculnya berita yang viral di dunia maya terkait keberadaan seorang perempuan yang fotonya termuat dalam sebuah poster dengan memakai kaos putih bergaris hitam dan dalam poster tersebut dibawah foto terdapat tulisan “Dengan ini saya menyatakan bahwa saya rela digilir seharga Rp 1.054.000 untuk melunasi hutang saya di aplikasi INCASH. Dijamin puas”. Dalam poster itu juga tercantum nomor ponsel YI<sup>9</sup>. Berita tersebut disebar oleh P2PL ilegal ke semua nomor kontak yang ada pada *hand phone* YI. Hal ini merupakan bukti lain yang menunjukkan adanya perilaku “nakal” *platform* P2PL yang mempunyai akses untuk memperoleh data pribadi nasabah khususnya foto dan nomor kontak *hand phone* dan menyalahgunakannya untuk kepentingan usaha. Kemudahan *platform* untuk mengakses data pribadi tersebut disebabkan karena pada saat *borrower* meng-*install*

<sup>5</sup> Taufik Hidayatullah, (2019), *Portal perlindungan nasabah fintech dari OJK*, Available online from <https://lokadata.id/artikel/ojk-segera-luncurkan-portal-perlindungan-konsum-en-fin-tech>, [Accessed Feb 02, 2021].

<sup>6</sup> Agustinus Respati, (2019), *Ada 4.500 Aduan Pinjaman Fintech yang Masuk ke LBH Jakarta*, Kontan.co.id, Available online from <https://keuangan.kontan.co.id/news/per-juni-2019-ada-4500-aduan-pinjaman-fintech-yang-masuk-ke-lbh-jakarta> [Accessed Feb 02, 2021].

<sup>7</sup> Syaiful Millah, (2019), *1.325 Aplikasi Android Ambil Data Pengguna Meski Tak Diberi Akses*, detik.com, Available online from <https://teknologi.bisnis.com/read/20190709/280/1121980/1.325aplikasi-android-ambil-data-pengguna-meski-tak-diberi-akses>, [Accessed Feb 02, 2021].

<sup>8</sup> Adhi Wicaksono, (2019), *Safenet Ungkap 3 Motif Pencurian Data Pribadi*, CNN Indonesia, Available online from <https://www.cnnindonesia.com/teknologi/20190801173431-185417499/safenet-ungkap-3-motif-pencurian-data-pribadi>, [Accessed Feb 02, 2021].

<sup>9</sup> Muhammad Hendartiyo, (2019), *Viral Wanita Relu Digilir terkait Fintech, Ini Kata Satgas SWI*, tempo.co, Available online from <https://bisnis.tempo.co/read/1228129/viral-wanita-relu-digilir-terkait-fintech-ini-kata-satgas-swi/full&view=ok>, [Accessed Feb 02, 2021].

aplikasi yang disediakan oleh *platform P2PL*, *platform* tersebut selalu meminta untuk diberikan akses terhadap semua nomor kontak yang ada di *hand phone borrower*.

Berdasarkan pada fakta tersebut perlindungan data pribadi pada transaksi P2PL merupakan suatu hal yang penting untuk dikaji dan ditemukan landasan konstitusionalnya agar semua pihak memahami pentingnya perlindungan data pribadi dan keberadaannya mempunyai landasan hukum yang kuat. Pembentukan peraturan perundang-undangan memerlukan landasan konstitusional baik formil maupun materiil sebagai dasar legitimasi peraturan tersebut<sup>10</sup>. Landasan konstitusional merupakan hal yang penting dan harus ada dalam peraturan perundang-undangan. Tulisan ini berupaya menjelaskan tentang landasan konstitusional perlindungan data pribadi pada transaksi *fintech lending*.

## **B. Permasalahan**

Dalam negara yang menganut pada prinsip negara hukum seperti Indonesia setiap penetapan peraturan atau kebijakan yang dibuat oleh penyelenggara negaramemerlukan landasan konstitusional yang berfungsi sebagai dasar legitimasi peraturan maupun kebijakan tersebut. Pentingnya landasan konstitusional mengharuskan setiap peraturan atau kebijakan mempunyai landasan konstitusional sehingga peraturan atau kebijakan tersebut mempunyai daya ikat yang kuat untuk dijadikan sebagai pijakan atau pedoman dalam setiap aktifitas kehidupan berbangsa dan bernegara. Berdasarkan pada pandangan tersebut terkait dengan perlindungan data pribadi dapat dirumuskan sebuah permasalahan apakah landasan konstitusional perlindungan data pribadi pada transaksi *fintech lending* di Indonesia?

## **C. Metode Penelitian**

Penelitian ini merupakan penelitian yuridis normatif dengan menggunakan pendekatan undang-undang (*statute approach*). Sumber data berasal dari data sekunder yang berupa data bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer dalam penelitian hukum berupa peraturan perundang-undangan yang otoritatif (berwibawa). Sedangkan bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan atau tambahan terhadap bahan hukum primer, seperti buku, artikel atau jurnal ilmiah, dan hasil penelitian yang berkaitan dengan topik penelitian. Analisis data dilakukan dengan menggunakan analisis deskriptif dengan pola pikir deduktif.

## **D. Pembahasan**

Perkembangan teknologi informasi yang pesat dewasa ini memberikan pengaruh yang luar biasa terhadap kehidupan manusia. Perkembangan teknologi informasi tersebut kemudian mempunyai dampak negatif disamping juga mempunyai dampak positif. Dampak positif yang ditimbulkan oleh teknologi informasi antara lain memudahkan orang untuk berinteraksi secara langsung melalui media internet. Akan tetapi kemudahan tersebut telah menciptakan efek negatif berupa penyalahgunaan data pribadi. Perlindungan hukum terhadap data pribadi penting untuk dipikirkan mengingat begitu cepatnya pertumbuhan teknologi telah memberikan kemudahan bagi para pihak dalam melakukan pengumpulan, analisa maupun menyebarkan informasi dengan berbagai cara<sup>11</sup>. Sebuah data akan dikategorikan sebagai data pribadi manakala data

---

<sup>10</sup> Evi Noviawati, 2018, *Landasan Konstitusional Pembentukan Peraturan Perundang-Undangan*, Jurnal Ilmiah Galuh Justisi Volume 6 Nomor 1, Hal. 53 – 63, DOI: <http://dx.doi.org/10.25157/jigj.v6i1.1246>

<sup>11</sup> Sinta Dewi, 2016, *Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia*, Jurnal Yustisia, Volume 5 No. 1 2016, Hal. 22 – 30, DOI: <https://doi.org/10.20961/yustisia.v5i1.8712>

tersebut berkaitan dengan seseorang yang dengannya orang tersebut dapat diidentifikasi sebagai pemilik data<sup>12</sup>. Definisi ini sejalan dengan pengertian data pribadi yang dilansir oleh OECD (*Organisation for Economic Co-operation and Development*) sebagaimana dikutip Siti Yuniarti, data pribadi merupakan segala informasi yang berkaitan dengan yang diidentifikasi atau individu dapat diidentifikasi dengannya<sup>13</sup>. Pengertian data pribadi secara normatif disebutkan dalam Pasal 1 (22) Undang-Undang Administrasi Kependudukan (UU. No. 23 tahun 2006 yang diubah dengan UU. No. 24 tahun 2013) bahwa Data pribadi adalah data yang dimiliki oleh orang yang menyimpan, merawat dan memelihara, serta dijaga kerahasiaannya.

Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Pada Sistem Elektronik No. 20 tahun 2016 juga memberikan pengertian data pribadi dengan definisi yang sama. Data perseorangan yang dimaksud dalam pengertian tersebut adalah segala keterangan yang dianggap mengandung kebenaran dan nyata menjadi satu kesatuan dengan diri seseorang serta dapat diidentifikasi secara langsung maupun tidak langsung pada setiap individu. Pengertian data pribadi yang berbeda dengan pengertian di atas disebutkan dalam Pasal 1 angka 29 Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP. No. 71 tahun 2019), yang menyatakan bahwa Data pribadi adalah data setiap orang yang secara langsung atau tidak langsung diidentifikasi melalui sistem elektronik dan atau non-elektronik dan atau diidentifikasi secara individu atau digabungkan dengan informasi lain. Kedua pengertian data pribadi tersebut mempunyai persamaan bahwa data pribadi merupakan data atau segala informasi yang melekat pada diri seseorang yang dengannya seseorang dapat diidentifikasi.

Penjelasan tentang jenis data pribadi tertuang dalam Pasal 28 Undang-Undang Administrasi Kependudukan (UU. No. 23 tahun 2006 yang diubah dengan UU. No. 24 tahun 2013), yang menyebutkan bahwa Data pribadi meliputi; Nomor Kartu Keluarga (KK), Nomor Induk Kependudukan (NIK), Nama Lengkap, Jenis Kelamin, Tempat Lahir, Tanggal, Bulan, Tahun Lahir, Golongan Darah, Agama/Keyakinan, Status Perkawinan, Status Hubungan Keluarga, Cacat Fisik dan Psikologi, pendidikan terakhir, jenis pekerjaan, NIK ibu kandung, nama ibu kandung, NIK ayah, nama ayah, alamat lama, alamat sekarang, kepemilikan akta kelahiran/akta kelahiran, nomor akta kelahiran/nomor akta kelahiran, akta nikah/akta nikah, nomor akta nikah/buku nikah, tanggal nikah, kepemilikan akta cerai, nomor akta cerai/akta cerai, tanggal cerai, sidik jari, iris mata, tanda tangan, dan elemen data lain yang merupakan aib pribadi.

Dalam RUU Perlindungan Data Pribadi (Pasal 3) disebutkan dua macam data pribadi yaitu data yang bersifat umum dan bersifat spesifik. Data pribadi yang bersifat umum mencakup nama lengkap seseorang, jenis kelamin, kebangsaan, keyakinan agama, dan data pribadi, yang dapat digabungkan untuk mengidentifikasi seseorang. Sementara itu, data pribadi spesifik mencakup data dan informasi kesehatan, data biometrik, data genetik, kehidupan atau orientasi seksual, opini politik, catatan kriminal, data anak, data keuangan pribadi, dan data lain yang sesuai dengan undang-undang dan peraturan.

Data pribadi yang melekat pada diri seseorang merupakan salah satu hak yang harus dilindungi. Data pribadi merupakan bagian dari privasi seseorang. Secara umum

---

<sup>12</sup> Sugeng, *Hukum Telematika Indonesia*, Kencana, Jakarta, 2020, Hal. 56

<sup>13</sup> Siti Yuniarti, 2019, *Perlindungan Hukum Data Pribadi Di Indonesia*, Jurnal Becoss (Business Economic, Communication, and Social Sciences), Vol.1, No.1 September 2019, Hal. 147-154, DOI: <https://doi.org/10.21512/becossjournal.v1i1.6030>



terdapat tiga aspek dalam privasi, yaitu privasi yang terkait dengan diri seseorang, privasi tentang data seseorang dan privasi atas komunikasi seseorang<sup>14</sup>. Penggunaan data oleh seseorang oleh pemerintah maupun swasta, badan usaha maupun perseorangan tanpa ijin merupakan pelanggaran privasi seseorang<sup>15</sup>. Oleh karenanya data pribadi harus dilindungi. Keharusan untuk melindungi data pribadi ini tercermin dalam Undang-Undang Dasar 1945 Pasal 28 G ayat 1 “*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*”. Ketentuan pasal tersebut semakna *Universal Declaration of Human Rights* yang tertuang dalam artikel 12 yang kemudian diadopsi dalam *International Covenant on Civil and Political Rights* (artikel 17) yang berlaku berdasarkan Undang-Undang No. 12 tahun 2005 memberikan hak atau jaminan pada perlindungan data pribadi.

Berdasar pada hal tersebut berarti konstitusi telah mengamankan untuk memberikan perlindungan terhadap data pribadi, oleh karenanya data pribadi yang berada pada instansi pemerintah baik pemerintah pusat maupun pemerintah daerah, lembaga-lembaga Negara, badan hukum pemerintah maupun swasta, atau institusi apapun dan dimanapun harus dijaga kerahasiaannya dan tidak dapat disebarluaskan tanpa ada izin dari pemilik data yang bersangkutan. Keharusan untuk melindungi data pribadi juga tercermin dalam Pasal 29 ayat 1 Undang-Undang HAM (UU. No. 39 tahun 1999) bahwa “*setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya*”. Terbitnya Peraturan Menteri Dalam Negeri tentang persyaratan, ruang lingkup dan prosedur pemberian akses dan penggunaan nomor identifikasi, data kependudukan dan Kartu Tanda Penduduk elektronik (Permendagri No. 61 tahun 2015) sangat berpotensi melanggar ketentuan UUD 1945 Pasal 28 G ayat 1, Undang-Undang No. 12 tahun 2005 dan Undang-Undang No. 39 tahun 1999 tentang Hak Asasi Manusia. Terbitnya Permendagri tersebut merupakan aturan pelaksana dari Undang-Undang Administrasi Kependudukan (Pasal 83 ayat 3) yang memberikan akses kepada masyarakat untuk memanfaatkan data penduduk yang dalam hal ini terkait dengan data pribadi.

Keberadaan RUU Perlindungan Data Pribadi yang sekarang berada di tangan Dewan Perwakilan Rakyat masih mempunyai celah penyalahgunaan data pribadi karena memberikan wewenang kepada pemerintah sebagai pengawas padahal Permendagri No. 61 tahun 2015 tersebut diatas merupakan tindakan pemerintah yang memberikan ijin kepada pihak-pihak yang telah bekerjasama dengan Kementerian Dalam Negeri untuk mengakses data pribadi. Oleh karenanya, perlu dibentuk lembaga independen yang melakukan pengawasan terhadap penyalahgunaan data pribadi sebagai hak dasar manusia yang dijamin dan mempunyai landasan yang kuat dalam UUD 1945.

Keberadaan Undang-Undang perlindungan data pribadi sangat diperlukan dalam rangka memberikan jaminan bahwa data pribadi dilindungi keberadaannya sehingga tidak disalahgunakan terlebih pada era teknologi informasi yang *disruptive* seperti sekarang ini. Hal ini penting untuk diwujudkan oleh pemerintah mengingat selama ini meskipun sudah ada beberapa peraturan yang berkaitan dengan data pribadi namun belum mampu melindungi data pribadi seseorang karena secara formalistik diberlakukan dalam bentuk peraturan dibawah undang-undang sehingga tidak memuat

---

<sup>14</sup> Edmon Makarim, *Pengantar Hukum Telematika*, Raja Grafindo Persada, Jakarta, 2005, Hal. 160

<sup>15</sup> Harun Mukhtar, *Kriptografi Untuk Keamanan Data*, Deepublish, Sleman, 2018, Hal. 8

ancaman hukuman yang mampu memberikan rasa jera terhadap pelaku yang menyalahgunakan data pribadi<sup>16</sup>.

Peraturan Otoritas Jasa Keuangan POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi sebagai payung hukum transaksi P2PL menyebutkan bahwa penyelenggara atau *platformfintech lending* harus menjaga kerahasiaan dan keutuhan serta ketersediaan data pribadi konsumennya yang pemanfaatannya harus memperoleh persetujuan dari pemilik data pribadi (Pasal 26). *Platform fintech lending* yang melanggar ketentuan dapat dikenakan sanksi administratif, denda, pembatasan usaha, dan pencabutan izin, namun ketentuan pasal ini tidak berlaku terhadap *platformfintech lending* ilegal yang tidak tunduk pada ketentuan tersebut. Hal tersebut disebabkan karena POJK No. 77/2016 hanya mengikat *platform fintech lending* yang telah terdaftar atau mendapat izin dari Otoritas Jasa Keuangan. Demikian pula halnya dengan Pasal 30 dan Pasal 31 Peraturan Otoritas Jasa Keuangan No. 13 /POJK.02/2018 tentang Inovasi Keuangan Digital tidak akan menjangkau penyalahgunaan data pribadi oleh *fintechlending* ilegal yang masih menjalankan kegiatan usahanya.

Pasal 2 (d) Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen Sektor Jasa Keuangan (POJK No. 1/POJK.07/2013) yang ditindaklanjuti dengan Surat Edaran tentang Kerahasiaan dan Keamanan Data dan atau Informasi Konsumen (SE OJK No.14/SEOJK.07/2014) yang menegaskan prinsip dasar perlindungan konsumen sesuai dengan prinsip kerahasiaan dan keamanan data atau informasi konsumen, dan merinci informasi pribadi konsumen, yang harus berupa nama, alamat, nomor telepon, tanggal lahir atau umur, dan data nama Rahasia atau informasi pribadi ibu kandung, karena POJK dan SEOJK tersebut belum memasukkan *fintech lending* sebagai pelaku usaha jasa keuangan.

Undang-Undang No. 11 tahun 2008 yang terakhir diubah dengan UU. No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yang menjadi pijakan pihak-pihak yang melakukan transaksi elektronik juga tidak memuat aturan tentang perlindungan data pribadi secara khusus. Dalam Pasal 26 (1) hanya menyebutkan bahwa “kecuali ditentukan lain oleh peraturan perundang-undangan” penggunaan data pribadi harus memperoleh persetujuan orang yang bersangkutan (pemilik data pribadi). Data pribadi merupakan salah satu bagian dari hak pribadi (*privacy right*) yang jika digunakan oleh orang lain tanpa ijin orang yang bersangkutan selaku pemilik data pribadi maka atas pelanggaran hak ini pemilik data pribadi apabila merasa mengalami kerugian dapat mengajukan gugatan (Penjelasan Pasal 26).

Secara khusus, regulasi yang berkaitan dengan perlindungan data pribadi tertuang dalam Peraturan Menteri Komunikasi dan Informatika No. 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Dalam peraturan tersebut diatur tentang cara perolehan, pengolahan dan menganalisis samapai pada bagaimana memusnahkan data pribadi. Dalam Permenkominfo tersebut juga mengatur kewajiban para pengguna dan penyelenggara sistem elektronik akan tetapi peraturan menteri ini tidak mempunyai “gigi” untuk menjerat pelaku yang menyalahgunakan data pribadi seseorang karena keberlakuannya yang hanya berdasarkan pada peraturan menteri tidak memuat sanksi yang mampu menjerakan terhadap pelanggar data pribadi. Sanksi bagi orang yang melanggar perlindungan terhadap data pribadi hanya berupa peringatan lisan

---

<sup>16</sup> Ada beberapa peraturan perundang-undangan yang terkait dengan perlindungan data pribadi antara lain tertuang dalam kliklegal.com, Ini Berbagai Peraturan Perlindungan Data Pribadi di Indonesia, <https://kliklegal.com/ini-berbagai-peraturan-perlindungan-data-pribadi-di-indonesia/>

dan tertulis, menghentikan kegiatan usaha yang bersifat sementara dan pengumuman pada *website online*. Hukuman ini tentu tidak mampu memberikan rasa jera bagi mereka yang melanggar ketentuan perlindungan data pribadi termasuk tidak menjerakan *platformfintech lending*.

Data pribadi yang melekat pada seseorang merupakan hak dasar yang harus dilindungi hukum dalam rangka meneggapai tujuan hukum yaitu keadilan, kepastian dan kemanfaatan, sebagaimana dinyatakan oleh Gustav Radbruch bahwa hukum harus mampu mengayomi hak dasar manusia yang dirugikan oleh orang lain<sup>17</sup>. Pemberian perlindungan Negara terhadap hak pribadi dapat meningkatkan nilai-nilai kemanusiaan dan hubungan antara individu dengan masyarakat serta dapat membatasi kekuasaan pemerintah<sup>18</sup>. Oleh karenanya, perlindungan data pribadi penting untuk diwujudkan dalam era teknologi informasi ini.

Berdasarkan pada hal tersebut, pertumbuhan transaksi *fintech lending* yang berbasis pada teknologi informasi yang dalam transaksinya selalu menggunakan data pribadi memerlukan sistem hukum atau regulasi dalam bentuk undang-undang yang mampu melindungi keamanan data pribadi aktornya. Hal tersebut perlu dilakukan mengingat ketentuan Pasal 28D ayat (1) UUD 1945 yang menyebutkan bahwa “*Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum*”. Ketentuan ini merupakan jaminan Negara terhadap hak dasar warga negara, jaminan dan perlindungan dari negara kepada setiap warga Negara akan meningkatkan taraf hidup warga Negara dan terlindungi privasinya. Dalam kaitan ini Roscoe Pound menyatakan bahwa hukum harus mampu menjalankan fungsinya untuk melindungi kepentingan umum, kepentingan sosial maupun kepentingan pribadi yang didalamnya termasuk perlindungan terhadap hak pribadi (*privacy*). Untuk melindungi kepentingan-kepentingan tersebut agar berjalan secara harmonis Roscoe Pound menawarkan teori *law as a tool of social engineering* sebagai perwujudan teori kepentingan. Menurut Pound, hukum merupakan media dinamis yang dapat memfasilitasi kohesi sosial yang ada dalam masyarakat melalui berbagai macam cara sehingga semua aspirasi masyarakat dapat terpenuhi yang dilakukan dengan menggunakan pendekatan *multi faceted* (beraneka segi) dan *multi stage* (beraneka tingkatan). Untuk mewujudkan hal tersebut menurut Pound dapat dilakukan melalui beberapa langkah, *pertama*, apa yang menjadi kepentingan (*interest*) masyarakat harus ditemukan dan ditetapkan sedemikian rupa. *Kedua*, melakukan inventarisasi dan klasifikasi terhadap kepentingan tersebut. *Ketiga*, bila terjadi konflik kepentingan diselesaikan melalui harmonisasi dan penyeimbangan<sup>19</sup>.

Dalam upaya memberikan perlindungan dan kesejahteraan bagi para pihak khususnya konsumen *fintech lending*, negara harus membuat regulasi atau seperangkat peraturan yang dapat menjamin kepastian hukum sesuai dengan kehidupan masyarakat dalam menghadapi nilai-nilai baru<sup>20</sup>. Di era teknologi, keamanan bertransaksi menjadi sangat penting karena keberadaannya dapat membangun kepercayaan bagi konsumen dan pelaku bisnis. Dalam rangka memperkuat posisi tawar konsumen dan menjamin kepastian hukum dalam bertransaksi, maka perlu dibentuk regulasi yang melindungi

<sup>17</sup>Dalam Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000, Hal.55

<sup>18</sup> Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi: Regulasi dan Konvergensi*, Refika Aditama, Bandung, 2010, Hal. 4

<sup>19</sup>Dalam Atip Latipulhayat, 2014, *Khazanah: Roscoe Pound*, Pajajaran Jurnal Ilmu Hukum, volume 1 No. 2 tahun 2014, Hal., 413 - 424, DOI: <https://doi.org/10.22304/pjih.v1n2.a12>

<sup>20</sup>Lili Rasjidi dan I.B Wyasa Putra, *Hukum sebagai Suatu Sistem*. Mandar Maju, Bandung, 2003, Hal. 187



konsumen dalam bertransaksi menggunakan sarana elektronik<sup>21</sup>. Salah satu bentuk perlindungan konsumen adalah perlindungan terhadap data pribadi sehingga hak konsumen terlindungi dan mempunyai kepastian hukum.

Kepastian hukum merupakan salah satu ajaran dalam cita hukum (*idee des recht*) yang terdiri dari kepastian hukum (*rechmatigheit*), keadilan (*gerechtigkeit*) dan kemanfaatan (*doelmatigheit*)<sup>22</sup>. Ketiga cita hukum tersebut secara proporsional harus ada dalam sistem hukum yang berlaku agar kehidupan masyarakat yang adil dan makmur dapat terwujud secara harmonis sebagaimana amanat Pembukaan UUD 1945 yang berfungsi sebagai landasan filosofis bangsa dan negara yang menganut pada prinsip negara hukum. Dalam negara hukum, pemerintah mempunyai kewajiban untuk mewujudkan keadilan dan kesejahteraan, sebagaimana dinyatakan oleh Aristoteles bahwa negara harus memberikan jaminan terwujudnya keadilan terhadap setiap warga negara<sup>23</sup>. Oleh karenanya, perundang-undangan yang ada (*ius constitutum*) dan hukum yang akan ada (*ius constituendum*) harus diwujudkan guna mewujudkan keadilan. Jika dikaitkan dengan konsep hukum progresif, semua peraturan yang menghalangi terwujudnya keadilan harus ditinggalkan.

Pada transaksi *fintech lending*, data pribadi peminjam (*borrower*) dan pemberi pinjaman (*lender*) tetap merupakan hak privasinya yang harus dilindungi. Platform *fintech lending* tidak boleh menyebarluaskan data pribadi yang mereka kuasai untuk kepentingan di luar proses transaksi *fintech lending*, karena data pribadi tersebut merupakan hak privasi seseorang yang keberadaannya dijamin oleh UUD 1945. Penjelasan Pasal 26 ayat 1 UU. ITE menyebutkan bahwa Negara merupakan pelaksana kedaulatan rakyat yang harus memberikan jaminan perlindungan terhadap warga negara atas penyalahgunaan data pribadi. Ada beberapa alasan pentingnya perlindungan terhadap data pribadi;

- a. Mencegah seseorang berpura-pura menjadi kamu (*phising*);
- b. Melindungi data finansial;
- c. Menghindari pencurian dan perampokan dengan perantara dan dukungan teknologi informasi;
- d. Menghindari Kekerasan Berbasis Gender Online (KBGO) seperti *cyber grooming* (memperdaya), pelecehan *online*, peretasan atau *hacking*, pelanggaran privasi, ancaman distribusi foto atau video pribadi serta pencemaran nama baik.

Pada era teknologi informasi, menjamin keamanan data pribadi sebagai sebuah informasi merupakan hal yang harus dilakukan, antara lain dengan menerapkan model CIA (*Confidentiality*, yang diarahkan untuk memberikan perlindungan terhadap informasi agar tidak diakses oleh pihak-pihak yang tidak berkepentingan. *Integrity*, yang dilakukan untuk melindungi informasi agar tidak dirubah oleh orang yang tidak bertanggungjawab. *Availability*, memberikan hak kepada pihak yang berwenang untuk mengakses informasi pada saat dibutuhkan)<sup>24</sup>.

---

<sup>21</sup>Liany Dewi Sanjoto, 2019, *Perlindungan Hukum Bagi Konsumen Pemakai Jasa Elektronik Dalam Transaksi Melalui Marketplace*, Jurnal Dunia Hukum, Volume 3 No. 2 April 2019, Hal. 95 – 112, DOI: <http://dx.doi.org/10.35973/jidh.v3i2.1365>

<sup>22</sup>Teori ini dikemukakan oleh Gustav Radbruch (1878-1949)

<sup>23</sup>Dalam Moh. Kusumohamidjojo dan Harmaily Ibrahim, *Pengantar Hukum Tata Negara Indonesia*, PSHTN FH UI dan Sinar Bakti, Jakarta, 1988, Hal. 153

<sup>24</sup>Soediro, 2018, *Prinsip Keamanan, Privasi dan Etika Dalam Undang-Undang ITE Dalam Perspektif Hukum Islam*, Jurnal Kosmik Hukum, Volume 18 No. 2 Juni 2018, Hal. 1 – 18, DOI: [10.30595/kosmikhukum.v18i2.3439](https://doi.org/10.30595/kosmikhukum.v18i2.3439)

*Confidentiality* terkait dengan keharusan *platform P2PL* untuk menyimpan data para nasabahnya dengan menerapkan prinsip *internal use only* dan melakukan enkripsi<sup>25</sup> pada data pribadi yang masuk pada *server*-nya. Untuk menjamin adanya *confidentiality* tersebut *platform P2PL* juga perlu melakukan literasi pada para nasabahnya untuk membuat password yang kuat (*password strength*) dan untuk tidak mudah percaya pada orang lain (*attacker*) dalam menggunakan teknologi informasi.

*Integrity* dilakukan untuk memastikan bahwa setiap data yang masuk ke *server* tetap terjaga akurasi, konsistensi dan validitasnya sehingga tidak dapat dirubah dan terjaga dari ancaman-ancaman yang muncul karena kesengajaan maupun maupun tidak disengaja. Untuk menjaga integritas data dapat menerapkan beberapa hal;

- a. Menerapkan enkripsi yang kuat pada media penyimpanan data;
- b. Menerapkan validasi yang kuat (*strong validation*) untuk memberikan jaminan legalitas akses yang dilakukan;
- c. Perhatian terhadap *access control* sehingga tidak semua orang dapat mengakses data yang disimpan.

*Availability* merupakan sebuah cara yang dilakukan untuk menjamin bahwa data siap untuk diakses saat kapanpun dan dimanapun. Untuk memastikannya setiap perusahaan dapat menerapkan beberapa hal, antara lain<sup>26</sup>;

1. Mempunyai *disaster recovery plan*;
2. Mempunyai banyak *power supply*;
3. Melakukan *backup* data secara rutin.

Penerapan model tersebut diharapkan mampu mengantisipasi adanya tindakan atau upaya yang bertujuan untuk pengambilan, pengubahan dan pengaksesan data pribadi tanpa ijin. Upaya yang dilakukan untuk mengambil atau melakukan pencurian data tanpa ijin merupakan salah hal yang dapat dikategorikan sebagai *cybercrime*.

## **E. Penutup**

Berdasarkan analisa diatas dapat diambil simpulan bahwa landasan konstitusional perlindungan data pribadi terletak pada keberadaan data pribadi sebagai hak dasar yang melekat pada diri manusia dan dijamin oleh UUD 1945 dan peraturan perundangan yang lain seperti UU. HAM dan UU. ITE. Peraturan perundangan yang terkait dengan transaksi *fintech lending* atau *peer to peer lending* belum memberikan perlindungan terhadap keamanan data pribadi konsumen terutama data pribadi *borrower* yang sering disalahgunakan. Oleh karenanya, untuk memberikan jaminan perlindungan terhadap data pribadi dalam transaksi *peer to peer lending*, *platform fintech lending* harus menerapkan model CIA (*confidentiality, integrity, dan availability*).

Mengacu pada simpulan tersebut sebagai saran terhadap pengambil kebijakan perlu dilakukan pembaharuan hukum melalui pembentukan regulasi dalam bentuk undang-undang yang melindungi data pribadi dalam transaksi *fintech lending* khususnya atau transaksi berbasis teknologi informasi pada umumnya. RUU Perlindungan Data Pribadi segera disahkan dengan melakukan penyesuaian terhadap perkembangan yang terjadi dan perlunya ada lembaga pengawas atau sejenisnya yang melakukan pengawasan terhadap penggunaan data pribadi.

---

<sup>25</sup>Enkripsi merupakan teknik untuk mengubah file, data atau informasi dari *plaintext* menjadi *chiphertext* sehingga tidak dapat dimengerti atau di-*hack* oleh orang lain.

<sup>26</sup> Bachrul Ilmi (2017), Mengenal CIA Triad - Prinsip Dasar IT Security, Bahrulilmi Available online from [http://www.bachrulilmi.com/2017/11/mengenal-cia-triad-prinsipdasar-itsecu\\_riety.html](http://www.bachrulilmi.com/2017/11/mengenal-cia-triad-prinsipdasar-itsecu_riety.html) [Accessed Feb 02, 2021].

## DAFTAR PUSTAKA

### Buku:

- Danrivanto Budhijanto. 2010. *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi: Regulasi dan Konvergensi*, Bandung: Refika Aditama
- Edmon Makarim. 2005. *Pengantar Hukum Telematika*, Jakarta: Raja Grafindo Persada
- Harun Mukhtar. 2018. *Kriptografi Untuk Keamanan Data*, Sleman: Deepublish
- Lili Rasjidi dan I.B Wyasa Putra. 2003. *Hukum sebagai Suatu Sistem*. Bandung; Mandar Maju
- Moh. Kusumohamidjojo dan Harmaily Ibrahim. 1988. *Pengantar Hukum Tata Negara Indonesia*, Jakarta: PSHTN FH UI dan Sinar Bakti
- Sugeng. 2020. *Hukum Telematika Indonesia*, Jakarta: Kencana
- Satjipto Raharjo. 2000. *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti

### Jurnal:

- Atip Latipulhayat. 2014. Khazanah: Roscoe Pound, *Pajajaran Jurnal Ilmu Hukum*, Volume 1 (2), 413 – 424, DOI: <https://doi.org/10.22304/pjih.v1n2.a12>
- Evi Noviawati. 2018. Landasan Konstitusional Pembentukan Peraturan Perundang-Undangan, *Jurnal Ilmiah Galuh Justisi* 6 (1), 53 – 63, DOI: [10.25157/jigj.v6i1.1246](https://doi.org/10.25157/jigj.v6i1.1246)
- Liany Dewi Sanjoto. 2019. Perlindungan Hukum Bagi Konsumen Pemakai Jasa Elektronik Dalam Transaksi Melalui Marketplace, *Jurnal Dunia Hukum*, 3 (2), 95 – 112, DOI: <http://dx.doi.org/10.35973/jidh.v3i2.1365>
- Sinta Dewi. 2016. Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia, *Jurnal Yustisia*, 5 (1), 22 – 30, DOI: <https://doi.org/10.20961/yustisia.v5i1.8712>
- Siti Yuniarti. 2019. Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal Becoss (Business Economic, Communication, and Social Sciences)*, 1 (1), 147-154, DOI: <https://doi.org/10.21512/becossjournal.v1i1.6030>
- Soediro. 2018 Prinsip Keamanan, Privasi dan Etika Dalam Undang-Undang ITE Dalam Perspektif Hukum Islam, *Jurnal Kosmik Hukum*, Volume 18 (2), 1 – 18, DOI: [10.30595/kosmikhukum.v18i2.3439](https://doi.org/10.30595/kosmikhukum.v18i2.3439)

### Internet:

- Agustinus Respati, (2019), Ada 4.500 Aduan Pinjaman Fintech yang Masuk ke LBH Jakarta, Kontan.co.id, Available online from <https://keuangan.kontan.co.id/news/per-juni-2019-ada-4500-aduan-pinjaman-fintech-yang-masuk-ke-lbh-jakarta> [Accessed Feb 02, 2021].
- Bachrul Ilmi (2017), Mengenal CIA Triad - Prinsip Dasar IT Security, Bahrulilmi Available online from <http://www.bachrulilmi.com/2017/11/mengenal-cia-triad-prinsipdasar-itsecurity.html> [Accessed Feb 02, 2021].
- Adhi Wicaksono, (2019), Safenet Ungkap 3 Motif Pencurian Data Pribadi, CNN Indonesia Available online from <https://www.cnnindonesia.com/teknologi/20190801173431-185417499/safenet-ungkap-3-motif-pencurian-data-pribadi>, [Accessed Feb 02, 2021].
- Muhammad Hendartiyo, (2019) Viral Wanita Rela Digilir terkait Fintech, Ini Kata Satgas SWI, tempo.co Available online from <https://bisnis.tempo.co/read/1228129/viral-wanita-rela-digilir-terkait-fintech-ini-kata-satgas-swi/full&view=ok>, [Accessed Feb 02, 2021].

Otoritas Jasa Keuangan RI, (2020), Data Statistik, OJK.go.id Available online from <https://www.ojk.go.id/id/kanal/iknb/data-danstatistik/fintech/Documents/Statistik%20Fintech%20Lending%20Desember%202020.pdf>, [Accessed Feb 02, 2021].

Syaiful Millah, (2018), 1.325 Aplikasi Android Ambil Data Pengguna Meski Tak Diberi Akses, Bisnsis.com Available online from <https://teknologi.bisnis.com/read/20190709/280/1121980/1.325aplikasi-android-ambil-data-pengguna-meski-tak-diberi-akses>, [Accessed Feb 02, 2021].

Taufik Hidayatullah, (2019), Portal perlindungan nasabah fintech dari OJK, Loka Data, Available online from <https://lokadata.id/artikel/ojk-segera-luncurkan-portal-perlindungan-konsumen-fintech>, [Accessed Feb 02, 2021].

### **Undang-Undang:**

Undang-Undang Dasar 1945

Undang-Undang Nomor 11 tahun 2008 yang terakhir diubah dengan Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 23 tahun 2006 yang terakhir diubah dengan Undang-Undang Nomor 24 tahun 2013 Tentang Administrasi Kependudukan

Undang-Undang No. 39 tahun 1999 tentang Hak Asasi Manusia

Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi

Peraturan Otoritas Jasa Keuangan No. 13 /POJK.02/2018 tentang Inovasi Keuangan Digital

Peraturan Menteri Dalam Negeri Nomor 61 tahun 2015 tentang Persyaratan, Ruang Lingkup dan Tata Cara Pemberian Hak Akses Serta Pemanfaatan Nomor Induk Kependudukan, Data Kependudukan dan Kartu Tanda Penduduk Elektronik

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