KRTHA BHAYANGKARA, Vol. 15, No. 1 (2021), pp. 11-38
ISSN 1978-8991 (print) | ISSN 2721-5784 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/KRTHA

Keamanan dan Akses Data Pribadi Penerima Pinjaman Dalam *Peer to Peer Lending* di Indonesia

Hendrawan Agusta
Pemerhati Teknologi Finansial (khusus *P2P Lending*)
Email: hagusta@yahoo.com

Article info

Received: Sep 13, 2020	Revised: Feb 20, 2021	Accepted: Feb 22, 2021	Published: Jun 10, 2021

DOI: https://doi.org/10.31599/krtha.v15i1.289

Keywords : *Personal Data, Data Security, Right of Access, Financial Tecnology, P2P Lending*

Abstract : *The development of information technology has changed the pattern of people's lives, one of which is bringing about a paradigm shift regarding new types of wealth so that the Data is The New Oil phenomenon appears. New business models that have emerged from the development of information technology have touched the financial industry and created financial technology, one of which is information technology-based lending and borrowing (Peer to Peer Lending/P2P Lending). Apart from creating opportunities through easy access to finance, P2P Lending also poses challenges related to Personal Data. Onc Borrower's Personal Data (Application User) enters the P2P Lending Operator's Electronic System, Borrower as the Data Subject will no longer have full control over their Personal Data. This research discusses Personal Data Security and Right of Access in P2P Lending. Personal Data Security plays an important role in preventing leakage of Personal Data, while Personal Data Access is a means for Borrower to exercise control over their Personal Data*

Kata kunci : Data Pribadi, Keamanan Data Pribadi, Akses Data Pribadi, Teknologi Finansial, *P2P Lending*

Abstrak : Perkembangan teknologi informasi telah merubah pola hidup masyarakat, salah satunya membawa perubahan paradigma mengenai jenis kekayaan baru sehingga muncul fenomena *Data is The New Oil*. Model bisnis baru yang muncul dari perkembangan teknologi informasi telah menyentuh industri keuangan dan melahirkan Teknologi Finansial, salah satunya pinjam-meminjam uang berbasis teknologi informasi (*Peer to Peer Lending/P2P Lending*). Selain melahirkan peluang melalui kemudahan mendapatkan akses keuangan, *P2P Lending* juga menimbulkan tantangan terkait Data Pribadi. Sekali Data Pribadi Penerima Pinjaman (Pengguna Aplikasi) masuk ke dalam Sistem Elektronik Penyelenggara *P2P Lending*, Penerima Pinjaman selaku Pemilik Data Pribadi tidak lagi memiliki kontrol penuh terhadap Data Pribadinya. Penelitian ini membahas Keamanan Data Pribadi dan Akses Data Pribadi dalam *P2P Lending*. Keamanan Data Pribadi memegang peranan penting untuk mencegah terjadinya kebocoran Data Pribadi, sedangkan Akses Data Pribadi merupakan sarana bagi Penerima Pinjaman untuk melakukan kontrol atas Data Pribadinya.

I. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat membawa perubahan paradigma mengenai jenis kekayaan baru. *Data is The New Oil* merujuk pada maksud bahwa sumber kekayaan alam yang paling berharga saat ini bukan lagi minyak, melainkan data. Dalam pidato kenegaraan pada tanggal 16 Agustus 2019, Presiden Jokowi menegaskan bahwa Indonesia harus bersiap dalam menghadapi ancaman penyalahgunaan data.[1] Presiden Joko Widodo menyebut dengan artikulasi yang sangat bernas bahwa Data adalah jenis kekayaan baru bangsa kita, kini data lebih berharga dari minyak[2]. The Economist menyebutkan bahwa "*a century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era*"[3].

Data adalah sumber daya penting yang menggerakkan ekonomi informasi seperti halnya minyak telah memicu ekonomi industri[4]. Semakin banyak data yang diproses dan diolah, maka semakin banyak hal-hal yang dapat disimpulkan dari proses tersebut, pada gilirannya didapatkan sebuah *output*, misalnya pola perilaku pembelian masyarakat, *appetite* masyarakat terhadap produk dan/atau jasa tertentu dan lain sebagainya. Data-data tersebut dikumpulkan menjadi sebuah kumpulan data yang besar (*Big Data*) yang menjanjikan sejumlah besar kegunaan baru untuk identifikasi, kemunculan bisnis baru dan sektor bisnis[5]. *Big Data* memberikan *input* yang vital bagi perekonomian dan memberikan landasan model bisnis baru. Virginia Rometty, salah satu petinggi IBM, sebuah perusahaan Amerika Serikat yang memproduksi dan menjual perangkat keras (*hardware*) dan perangkat lunak (*software*) komputer mengatakan bahwa *Big Data is The New Oil*[6], karenanya penulis menyimpulkan baik Data maupun *Big Data* merupakan fenomena *The New Oil* sebagai *game changer* bagi transaksi elektronik dunia, termasuk Indonesia

Minyak merupakan sumber daya mentah, baru bisa bermanfaat apabila sudah diolah menjadi produk tertentu, misalnya pelumas dan bensin. Analogi ini tepat untuk menggambarkan bahwa Data juga merupakan sumber daya mentah, baru bisa bermanfaat setelah diolah dan dianalisis sedemikian rupa melalui *Artificial Intelligence* untuk tujuan tertentu. *Data are analogous to raw material resources, which only acquire direct value in use, after they*

---

[1] Danrivanto Budhijanto, "Data As New Oil dalam Konstruksi Hukum Ekonomi Digital di Indonesia", https://www.hukumonline.com/berita/baca/, diakses 25 November 2019.

[2] *Ibid.*

[3] David Parkins,"The World's Most Valuable Resource Is No Longer Oil, But Data", https://www.economist.com/leaders/, diakses 25 November 2019.

[4] Dennis D. Hirsch, "The Glass House Effect: Big Data, The New Oil, and the Power of Analogy", *Maine Law Review* Vol. 66 No. 2 (Juni 2014), hlm. 374.

[5] *Ibid.*

[6] *Ibid.*

are extracted and processed in specific ways[7]. Semakin banyak bisnis yang sadar akan pentingnya *Big Data* sebagai sumber strategi, dimana dengan menganalisa *history* pembelian konsumen, sebuah bisnis dapat dengan mudah mengidentifikasi tren dan pola kebutuhan konsumen. *More and more businesses are waking up to the importance of Big Data* as a *strategic resource*[8].

Berdasarkan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Perkominfo PDP), Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya[9]. Terhadap Data Pribadi, meskipun seseorang telah mengunggah Data Pribadi dalam aplikasi P2P Lending, namun kepemilikannya tidak ikut diserahkan, orang tersebut secara hukum masih sebagai *owner* atas Data Pribadinya. Tentu saja jika menganalisis mengenai Data Pribadi tidak cukup hanya melihat pada Perkominfo PDP, tapi juga harus dianalisis menggunakan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) berikut kecukupan aturan normatif lainnya.

Pemanfaatan *P2P Lending* menimbulkan tantangan terkait perlindungan Data Pribadi dalam setiap aspek pemrosesannya. Salah satu perlindungan Data Pribadi tersebut berkenaan bagaimana Data Pribadi tersebut akan diproses[10]. Keamanan Data Pribadi wajib diterapkan oleh Penyelenggara *P2P Lending* (selanjutnya disebut Penyelenggara) agar jangan sampai terjadi kebocoran Data Pribadi. Penyelenggara wajib melakukan langkah-langkah dan pendekatan teknologi untuk mencegah terhadinya kebocoran Data Pribadi yang jika terjadi dapat menimbulkan kerugian baik langsung maupun tidak langsung terhadap pemilik Data Pribadi. Seperti kita ketahui bahwa baru-baru ini terdapat kasus kebocoran Data Pribadi yang dialami Tokopedia, dimana terdapat 91 juta Data Pribadi pengguna aplikasi Tokopedia yang bocor dan diperdagangkan oleh pihak-pihak yang tidak bertanggungjawab, sehingga menimbulkan kemungkinan kerugian bagi pengguna aplikasi Tokopedia selaku Pemilik Data Pribadi. Kasus tersebut telah masuk ke ranah hukum di Pengadilan Negeri Jakarta Pusat dengan Komunitas Konsumen Indonesia (KKI) bertindak sebagai Penggugat, Menteri Komunikasi dan Informatika bertindak sebagai

---

[7] Michele Loi dan Paul Olivier Dehaye, "If Data Is The New Oil, When Is The Extraction of Value From Data Unjust", *Philosophy and Public Issues – Tyranny, Democracy, and* Economy Vol. 7 No. 2 (2017), hlm. 139.

[8] Noriko Higashizawa dan Yuri Aihara, "Data Privacy Protection of Personal Information Versus Usage of Big Data : Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)", *Defense Counsil Journal* Vol. 84 No. 4 (2017), hlm. 1.

[9] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronik,* Perkominfo No. 20 Tahun 2016, Ps. 1 angka (1).

[10] Sinta Dewi Rosadi, "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia", *Jurnal Veritas et Justicia* Vol. 4 No. 1 (2018), hlm. 88.

Tergugat I dan PT Tokkopedia bertindak sebagai Tergugat I, kasus tersebut disidangkan di bawah register Perkara No. 235/PDT.G/ 2020/PN.JKT.PST dengan klasifikasi Gugatan Perbuatan Melawan Hukum[11].

Penulis bukan bermaksud membahas kasus Tokopedia, melainkan hanya sebagai pengantar bahwa di Indonesia pernah terdapat kasus kebocoran Data Pribadi yang begitu menyita perhatian publik. Dalam penelitian ini penulis membuat batasan-batasan mengenai materi yang dianalisis. Batasan pertama, materi yang dibahas penulis terbatas pada keamanan Data Pribadi (*Data Security*) dan akses Data Pribadi (*Right of Access*) Data Pribadi Penerima Pinjaman (selaku pemilik Data Pribadi) dalam penyelenggaran *P2P Lending*. Adapun peristiwa kebocaran Data Pribadi yang dialami Tokopedia hanya penulis gunakan sebagai pengantar untuk mempertajam analisis mengenai pentingnya keamanan sistem elektronik dalam penyelenggaraan *P2P Lending*. Batasan kedua, penyelenggaraan *P2P Lending* yang dibahas terbatas pada penyelenggaraan *P2P Lending* yang terdaftar, baik terdaftar sistem elektroniknya pada Kementerian Komunikasi dan Informatika cq. Direktorat Jenderal Aplikasi dan Informatika (Ditjen Aptika) maupun yang terdaftar perizinannya di Otoritas Jasa Keuangan (OJK), sedangkan penyelenggaraan *P2P Lending* tidak terdaftar (tidak terdaftar sistem elektroniknya dan tidak terdaftar perizinanannya) tidak dibahas dalam penelitian ini.

Berdasarkan hal-hal tersebut di atas, berikut ini rumusan permasalahan yang akan dibahas dalam penelitian ini, yaitu (1) Bagaimana penerapan keamanan Data Pribadi Pengguna Aplikasi oleh Penyelenggara *P2P Lending* di Indonesia?. Dan (2) Bagaimana transaksi elektronik di Indonesia mengatur Akses Data Pribadi dalam penyelenggaraan *P2P Lending* ?

II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif atau penelitian hukum doktrinal, yaitu penelitian perpusatakaan atau studi dokumen karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum yang lain[12]. Penelitian doktrinal terdiri dari penelitian yang berupa usaha inventarisasi hukum positif, penemuan asas-asas dan falsafah (dogma atau doktrin) hukum positif, dan penemuan hukum *in concreto* yang layak diterapkan untuk

[11] Wahyunanda Kusuma Pertiwi,"Sidang Perdana Kasus Kebocoran Data Tokopedia Digelar Hari Ini", https://tekno.kompas.com/read/2020/06/10/09144017/, diakses 24 Agustus 2020.

[12] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, cet ke-8 (Jakarta : PT Raja Grafindo Persada, 2004), hal. 4.

menyelesaikan suatu perkara hukum tertentu[13].

Dalam penelitian ini teori yang akan digunakan sebagai pisau analisa adalah Teori Hak Kebendaan. Pasal 499 KUHPerdata memberikan definisi benda, yaitu tiap-tiap barang dan tiap-tiap hak yang dapat dikuasai oleh hak milik. Hak Kebendaan (*zakelijk recht*) adalah suatu hak yang memberikan kekuasaan langsung atas suatu benda, kekuasaan mana dapat dipertahankan terhadap tiap orang[14]. Hak Kebendaan itu meliputi benda yang berwujud dan benda yang tidak berwujud. Salah satu ciri Hak Kebendaan itu bersifat mutlak, dimana dalam hal ada gangguan oleh orang ketiga, pemilik hak benda dapat melaksanakan haknya terhadap siapapun juga[15].

Data Pribadi Pengguna Aplikasi yang dimasukkan dalam aplikasi P2P *Lending* yang kemudian disimpan dalam bentuk informasi elektronik merupakan Kebendaan Digital (*Digital Property*) yang dapat dikuasai oleh hak milik Pengguna Aplikasi selaku pemilik Data Pribadi. Kebendaan Digital memenuhi karakteristik tertentu, yaitu bersifat impersonal dan eksternal untuk manusia, memiliki kepentingan atas benda itu sendiri (kepentingan manusia untuk menguasai benda), merupakan kumpulan hak (hak untuk memakai, mengelola, mengalihkan dll), merupakan hak konstitusional dalam Pasal 17 Deklarasi HAM yang mengatur bahwa *everyone has the right to own property* dan merupakan hak absolut (mutlak) dalam artian dapat dipertahankan terhadap siapa saja yang mengganggunya[16]. Dengan kata lain, pemilik Data Pribadi mempunyai Hak Kebendaan atas Data Pribadinya yang disimpan Penyelenggara, salah satunya hak atas keamanan Data Pribadi dan hak untuk mengakses Data Pribadi.

Jenis dan data yang digunakan dalam penelitian ini adalah bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif, artinya mempunyai otoritas[17]. Bahan hukum primer terdiri dari perundang-undangan, risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim. Adapun bahan hukum sekunder berupa publikasi hukum, meliputi buku dan jurnal hukum. Setelah penulis mengumpulkan sumber bahan hukum, dalam penelitian ini penulis menggunakan pendekatan undang-undang (*statute approach*), yaitu dilakukan dengan menelaah semua undang-undang dan regulasi yang terkait dengan permasalahan

[13] E.Saefullah Wiradipradja, *Penuntun Praktis Metode Penelitian dan Penelitian Karya Ilmiah*, cet. 2, (Bandung : CV Keni Media, 2016), hal. 28.

[14] Subekti, *Pokok-Pokok Hukum Perdata*, (Jakarta : Intermasa, 1979), hlm. 52.

[15] Wirjono Prodjodikoro, *Azas-azas Hukum Perjanjian*, (Bandung : Sumur, 1993), hlm. 13-14.

[16] Abdul Salam, *Hukum Kebendaan Digital (Digital Property) : Kajian Hukum Keperdataan Terhadap Kebendaan Digital*, (Ringkasan Disertasi Doktorr Ilmu Hukum Universitas Indonesia, 2017), hlm. 41-47.

[17] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta : Prenadamedia Group, 2014), hlm. 181.

yang dianalisis. Penelitian ini adalah penelitian hukum normatif, sehingga metodenya analisa datanya bersifat kualitatif, tidak berbentuk angka[18].

III. PEMBAHASAN

A. Penerapan keamanan Data Pribadi oleh Penyelenggara *P2P Lending* di Indonesia

Penyelenggara wajib menerapkan suatu sistem manajemen pengamanan informasi untuk menjamin kerahasiaan dan keamanan Data Pribadi Pengguna Aplikasi *P2P Lending*. Kerahasiaan data (*Data Confidentiality*) ini berkaitan dengan konsepsi mengenai privasi yang dalam praktiknya berhubungan dengan data perserorangan tertentu, sedangkan keamanan data (*Data Security*) berkaitan dengan upaya yang dilakukan Penyelenggara *P2P Lending* dalam menerapkan prinsip-prinsip perlindungan Data Pribadi menggunakan pendekatan teknologi dan praktik bisnis yang mendukung untuk itu. Berdasarkan POJK No. 77, salah satu prinsip dasar bagi dari perlindungan Pengguna Aplikasi adalah kerahasiaan dan keamanan data[19]. Kerahasiaan dan keamanan Data Pribadi ini saling terkait satu sama lainnya, dimana kerahasiaan data sangat bergantung pada tingkat keamanan data. *The relationship between security and data privacy has always been complicated, privacy depends absolutely on security*[20].

Privasi adalah hak individu untuk menentukan apakah Data Pribadi akan dikomunikasikan atau tidak kepada pihak lain. Dalam pemanfaatan teknologi informasi, perlindungan Data Pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*)[21]. Hak pribadi mengandung pengertian : (a) hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, (b) hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai dan (c) hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Alasan privasi harus dilindungi, yaitu[22] pertama, dalam membina hubungan dengan orang, seseorang harus menutupi sebagian kehidupan pribadinya, sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. Kedua, seseorang di dalam

---

[18] E.Saefullah Wiradipradja, *Penuntun Praktis Metode Penelitian dan Penelitian Karya Ilmiah*, hlm. 28.

[19] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 29.

[20] Christopher Kuner, *et al.*, "The Rise Of Cybersecurity And Its Impact On Data Protection", *International Data Privacy Law* Vol. 7 No. 2 (2017), hlm. 73.

[21] Indonesia, *Undang-Undang Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, UU No. 19 Tahun 2016, TLN No. 5952, Penjelasan Ps. 26 ayat (1).

[22] Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* (Bandung : PT Refika Aditama, 2015, hlm. 16-17.

kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*) sehingga privasi sangat diperlukan oleh seseorang. Ketiga, privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain, akan tetapi hak ini akan hilang apabila seseorang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik, termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai *the right against the word*. Kelima, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik karena telah mengganggu kehidupan pribadinya, sehingga bila ada kerugian yang diderita, maka pihak korban wajib mendapatkan kompensasi.

Teori privasi modern dikembangkan pertama kali oleh Alan Westin dalam bukunya yang berjudul *Privacy and Freedom* yang berpendapat bahwa *privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to others*[23]. Definisi yang dikemukakan oleh Westin tersebut, kemudian dikembangkan oleh para pakar hukum lainnya terutama dalam menyikapi perkembangan dan kemajuan teknologi informasi dan komunikasi[24]. Westin telah membagi privasi ke dalam 4 (empat) jenis, yaitu[25] :

a. *Solitude*

   Keinginan untuk dapat menyendiri, seseorang diberi hak untuk dapat menyendiri dan bebas dari gangguan orang lain seperti bebas dari gangguan suara (*noises*), bau yang tidak sedap (*odours*) atau getaran keras (*vibration*).

b. *Intimacy* (kedekatan)

   Seseorang mempunyai hak untuk dapat melakukan hubungan yang sangat pribadi dengan orang-orang terdekat seperti hubungan kekeluargaan, hubungan antar suami-istri, hubungan kerja tanpa adanya gangguan dari pihak lain.

c. *Anonymity* (tidak dikenal)

   Hak ini menjadi dasar seseorang untuk tidak dikenal atau diketahui identitasnya dan seseorang tidak boleh diikuti gerak geriknya.

---

[23] Alan F. Westin, *Privacy and Freedom*, (London : Atheneum, 1967), hlm. 7 dalam Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* hlm. 18.

[24] *Ibid.*

[25] Solove dan Rotenberg, *Information Privacy Law*, (New York : Aspen Publication, 2006), hlm. 28 - 31 dalam Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* hlm. 19.

d. *Reserve* (adanya jarak)

Seseorang mempunyai hak untuk mengatur jarak antara kepentingan umum dengan kepentingan pribadinya sehingga seseorang bebas untuk menentukan apakah akan mengambil jarak atau tidak dengan publik.

Mengingat ruang lingkup yang sangat luas, maka beberapa pakar mencoba mempermudah mempelajari privasi dengan membagi dalam 4 (empat) kategori, yaitu[26]:

a. *Information privacy*

Privasi yang mengatur tentang pengumpulan dan pengelolaan data atau data privasi seperti informasi tentang keuangan dan informasi tentang kesehatan seseorang.

b. *Bodily privacy*

Privasi atas tubuh seseorang seperti privasi atas DNA, Data Biometrik seseorang, seperti retina mata dan sidik jari.

c. *Communication privacy*

Privasi atas komunikasi seseorang, seperti surat, telepon, email atau bentuk komunikasi lainnya.

d. *Territorial privacy*

Privasi atas tempat tinggal seseorang, tempat kerja.

Seluruh kategori privasi di atas jika dihubungkan dengan Data Pribadi Pengguna Aplikasi, dapat dianalisis satu persatu, pertama, Penyelenggara *P2P Lending* menyimpan data keuangan Pengguna Aplikasi mengenai jumlah pinjaman, status pinjaman (lunas atau gagal bayar) dan waktu jatuh tempo pinjaman. Data keuangan menurut Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP *update* Desember 2019) termasuk ke dalam Data Pribadi yang bersifat spesifik[27]. Kedua, Penyelenggara *P2P Lending* menyimpan data atas tubuh Pengguna Aplikasi berupa foto wajah yang melekat pula Data Pribadi lainnya seperti jenis rambut bisa berupa lurus, ikal, keriting, kasar, halus atau botak; bentuk wajah bisa berupa lonjong, oval atau kotak; bentuk mata bisa berupa bulat, sipit, mata naik, mata turun; bentuk tulang pipi; bentuk bibir bisa berupa tebal, tipis, atas tebal bawah tipis atau sebaliknya atas tipis bawah tebal. Pengguna Aplikasi yang telah mengunggah foto wajahnya ke dalam aplikasi *P2P Lending*, terdapat perekaman Data Pribadi yang tentu sangat berbahaya apabila disalahgunakan oleh Penyelenggara *P2P*

[26] Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* hlm. 19 -20.

[27] Ps. 3 ayat (3) RUU PDP mengatur bahwa Data Pribadi yang bersifat spesifik terdiri dari data dan informasi kesehatan, data biometrik, data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi dan/atau data lainnya sesuai ketentuan peraturan perundang-undangan.

Lending, apalagi ketika sudah masuk dalam sistem elektronik penyelenggara, pemilik data tidak lagi begitu mempunyai kontrol yang banyak atas datanya. *Once entered into any IT system such as government's or corporate database, personal information is not any more in strict control of its owner*[28]. Data Pribadi Pengguna Aplikasi yang disimpan dalam sistem elektronik merupakan Kebendaan Digital yang melekat padanya Hak Kebendaan, dimana setiap penggunaan data tersebut harus sesuai dengan tujuan yang spesifik dan atas persetujuan dari pemilik data, tidak boleh disalahgunakan untuk keperluan lainnya di luar tujuan yang telah disepakati.

Salah satu contoh potensi pelanggaran terhadap penyalahgunaan data adalah dalam program e-KTP yang menghendaki identitas tunggal penduduk agar dapat berlaku seumur hidup. Perekaman data meliputi informasi pribadi warga negara termasuk ciri-ciri fisik orang tersebut, antara lain pemindaian terhadap sidik jari dan retina mata yang digunakan untuk validasi bimoterik pemegang KTP[29]. Titik permasalahan terkait e-KTP adalah perihal *server* penyimpan data e-KTP merupakan milik negara lain, sehingga bank data yang dikumpulkan sangat rentan untuk diakses pihak asing dan tidak bertanggungjawab[30]. Dalam *P2P Lending*, terkait *server*, Kementerian Komunikasi dan Informatika RI (Kominfo) mensyaratkan bahwa untuk mendapatkan Sertifikat PSE, setiap Penyelenggara *P2P Lending*[31] wajib mempunyai *server* yang berlokasi di Indonesia[32]. OJK juga mensyaratkan hal yang sama bahwa Penyelenggara *P2P Lending* wajib menggunakan pusat data dan pusat pemulihan bencana yang ditempatkan di Indonesia[33]. Hal ini bertujuan agar data tersebut tidak disalahgunakan oleh pihak lain dan mendatangkan kerugian bagi pemilik Data Pribadi.

Ketiga, Penyelenggara *P2P Lending* menyimpan data percakapan dengan Pengguna Aplikasi, contohnya data percakapan saat proses penagihan pinjaman gagal bayar. Keempat, Penyelenggara *P2P Lending* menyimpan data Pengguna Aplikasi yang terdapat dalam KTP, yaitu nama, tempat tanggal lahir, alamat, agama, status perkawinan dan pekerjaan (data-data ini termasuk Data Pribadi yang bersifat umum). Penerima Pinjaman

---

[28] Dejan Z. Jankovic, "Key Security Measures For Personal Data Protection In IT Systems", *20th Telecommunications forum TELFOR 2012*, (Serbia, Belgrade, November 20-22, 2012), hlm. 79.

[29] Wahyudi Djafar, Bernhard Ruben Fritz Sunigar dan Blandina Lintang Setianti, *Perlindungan Data Pribadi : Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusi*, (Jakarta : Lembaga Studi dan Advokasi Masyarakat/ELSAM, 2016), hlm. 55.

[30] *Ibid.*

[31] Pendaftaran Sistem Elektronik Penyelenggara *P2P Lending* termasuk ke dalam kategori Pendaftaran PSE Non Penyelenggara Negara.

[32] https://layanan.kominfo.go.id/faqs

[33] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 25 ayat (1) dan (2).

yang gagal melakukan pembayaran seringkali didatangi oleh *debt collector* di tempat tinggalnya dan mendapat intimidasi menggunakan cara-cara yang melawan hukum, ini tidak diperbolehkan secara hukum. Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM), dalam Pasal 31 mengatur bahwa tempat kediaman seseorang tidak boleh diganggu, menginjak atau memasuki suatu pekarangan tempat kediaman atau memasuki suatu rumah bertentangan dengan kehendak orang yang mendiaminya, hanya diperbolehkan dalam hal-hal yang telah ditetapkan oleh undang-undang. Data Pribadi sebagaimana 4 (empat) kategori di atas disimpan dalam bentuk digital berupa informasi elektronik dan/atau dokumen elektronik dalam sistem elektronik dan dijaga kerahasiaannya sebagai salah satu kewajiban yang harus dipenuhi Penyelenggara *P2P Lending* berdasarkan Pasal 26 ayat (1) PP PSTE. Selain itu, terkait pelaksanaan kerahasiaan data, berdasarkan POJK No. 77, Penyelenggara *P2P Lending* wajib[34]:

a. Menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan;
b. Memastikan tersedianya proses autentikasi, verifikasi, dan validasi yang mendukung kenirsangkalan dalam mengakses, memproses, dan mengeksekusi data pribadi, data transaksi, dan data keuangan yang dikelolanya;
c. Menjamin bahwa perolehan, penggunaan, pemanfaatan, dan pengungkapan data pribadi, data transaksi, dan data keuangan yang diperoleh oleh Penyelenggara berdasarkan persetujuan pemilik data pribadi, data transaksi, dan data keuangan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
d. Menyediakan media komunikasi lain selain Sistem Elektronik Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi untuk memastikan kelangsungan layanan nasabah yang dapat berupa surat elektronik, call center, atau media komunikasi lainnya; dan
e. Memberitahukan secara tertulis kepada pemilik data pribadi, data transaksi, dan data keuangan tersebut jika terjadi kegagalan dalam perlindungan kerahasiaan data pribadi, data transaksi, dan data keuangan yang dikelolanya.

Penyelenggara *P2P Lending* sebagai Penyelenggara Sistem Elektronik harus menerapkan standar ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh

[34] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 26.

Instansi Pengawas dan Pengatur Sektornya[35]. ISO/IEC 27001 ini merupakan standar internasional yang disiapkan sebagai model untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan Sistem Manajemen Pengamanan Informasi. Penerapan standar ISO/IEC 27001 ini untuk memastikan perlindungan atas Data Pribadi Penerima Pinjaman (Pengguna Aplikasi) demi tercapainya keamanan informasi, yaitu terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi[36].

Setiap Penyelenggara *P2P Lending* yang telah terdaftar di OJK, selain wajib mendapatkan Sertifikat PSE dari Kominfo, juga wajib memperoleh sertifikasi ISO/IEC 27001 agar dapat lolos dalam tahap perizinan. Hal ini dinyatakan secara tegas saat OJK mengeluarkan Surat Tanda Terdaftar kepada setiap Penyelenggara *P2P Lending* dengan merujuk kepada ketentuan Pasal 28 ayat (2) Permenkominfo No. 4 Tahun 2016, yaitu "*pada saat Peraturan Menteri ini mulai berlaku, Penyelenggara Sistem Elektronik yang Sistem Elektroniknya baru beroperasi wajib dilakukan sertifikasi Sistem Manajemen Pengamanan Informasi paling lambat 1 (satu) tahun sejak beroperasinya Sistem Elektronik*".

Penulis menganalisis bahwa penerapan standar ISO/IEC 27001 merupakan bagian dari penerapan *Privacy by Design*, yaitu suatu teori yang menitikberatkan pada pendekatan teknologi dan praktik bisnis untuk mengatur data privasi[37]. Perlindungan Data Pribadi tidak cukup melalui regulasi peraturan perundang-undangan, akan tetapi juga harus diikuti oleh sistem teknologi informasi dan praktik bisnis Penyelenggara *P2P Lending* yang selalu melindungi dan memperhatikan hak-hak Pengguna Aplikasi dan infratsruktur yang mendukung, sehingga Penyelenggara *P2P Lending* dapat dipercaya sebagai *platform* aplikasi yang aman dalam memproses Data Pribadi. *Individuals want trustworthy behaviours throughout the ecosystem which extends beyond protecting privacy to encompass data security, data accuracy, the purpose for which data are used and any "code of ethics" that helps determine "appropriate" uses*[38]. Agar *Privacy by Design* dapat diterapkan secara efektif, maka harus mengggunakan Prinsip Dasar, yaitu[39] :

---

[35] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Sistem Manajemen Pengamanan Informasi,* Perkominfo No.4 Tahun 2016, Ps. 7.

[36] *Ibid*, Ps. 1 angka (6).

[37] Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, hlm. 21.

[38] World Economic Forum dan A.T. Kearney, *Rethinking Personal Data : A New Lens for Strengthening Trust*, Mei 2014, hlm. 12.

[39] http://www.privacybydesign.ca/index.php/about-pbd/landmark-resolution/ dalam Sinta Dewi Rosadi, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* hlm. 21.

a. Proaktif, artinya harus dipersiapkan semua alat, sarana, infrastruktur, praktik bisnis untuk melindungi data sebelum kerugian timbul.
b. *Default Setting*, artinya sistem dan infrastruktur harus secara otomatis dibuat untuk melindungi data.
c. *Design-embedded*, artinya perlindungan data disediakan dalam *design* IT dan ada dalam kebijakan perusahaan dan praktik bisnis.
d. Transparansi, yaitu adanya keterbukaan informasi kepada semua pengguna tentang sistem dan praktik bisnis yang digunakan.
e. *End to end security*, *Privacy by Design* yang telah tertanam ke dalam sistem sebelum elemen pertama dari informasi yang dikumpulkan, menjangkau seluruh siklus hidup data yang terlibat, dari awal sampai akhir. Hal ini memastikan bahwa pada akhir proses, semua data secara aman hancur, secara tepat waktu.
f. *Visibility and Transparancey-Keep it Open*, *Privacy by Design* yang berusaha untuk meyakinkan semua pihak bahwa setiap praktik bisnis atau teknologi yang terlibat sesuai dengan janji-janji dan tujuan yang dinyatakan. Bagian komponen dan operasi tetap terlihat dan transparan.
g. *Respect User*, yaitu menghargai pengguna dengan selalu memberikan informasi tentang kebijakan privasi dan kemudakan pengguna untuk dapat mengerti kebijakan privasi tersebut.

Keamanan Data Pribadi merupakan salah satu prinsip yang diatur dalam RUU PDP, Pengendali Data Pribadi[40] (Penyelenggara *P2P Lending* termasuk di dalamnya) wajib melindungi dan memastikan keamanan Data Pribadi yang dikelolanya meliputi penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan dan penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi. Aplikasi *P2P Lending* sebagai teknologi informasi yang memberikan *platform* komunikasi langsung antara orang yang satu dengan orang yang lain/P2P, dalam penerapannya selalu mengakses langsung informasi Data Pribadi orang yang memanfaatkan aplikasi tersebut. Semua hal yang berkaitan dengan teknologi informasi tidak dapat menjamin 100% perlindungan data, akan selalu ada celah. Penerapan ISO/IEC 27001 diharapkan dapat meminimalisir hal tersebut demi terjaganya kerahasiaan

[40] Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi (RUU PDP, Ps. 1 angka 3).

dan keamanan Data Pribadi Pengguna Aplikasi. *Many P2P application offer direct access to your information and services…the P2P applications could have security holes, or improper administrations could create one…P2P raises serius concerns, but nor activity or technology is 100 safe*[41].

Menurut penulis, Penyelenggara *P2P Lending* berdasarkan Pasal 4 Perkominfo No. 4 Tahun 2016 merupakan Penyelenggara Sistem Elektronik tingkat tinggi, alasannya ada 2 (dua), yaitu pertama, karena Penyelenggara *P2P Lending* diwajibkan mendapat Sertifikasi ISO/IEC 27001 dan kedua, karena aplikasi *P2P Lending* merupakan sistem elektronik yang berdampak pada kepentingan sektor tertentu, dalam hal ini sektor keuangan. Penilaian bahwa Penyelenggara *P2P Lending* merupakan Penyelenggara Sistem Elektronik tingkat tinggi ini, penulis analisis menggunakan tabel yang menjadi lampiran Perkominfo No. 4 Tahun 2016 dan mengambil contoh salah satu Penyelenggara *P2P Lending* dengan aplikasi *Cashcepat* (PT Artha Permata Makmur), sebagai berikut :

Tabel Kategori Sistem Elektronik *P2P Lending*

No	Karakteristik Sistem Elektronik	Bobot Nilai		
		A = 5	**B=2**	**C=1**
1	Nilai investasi sistem elektronik yang terpasang	Lebih dari 30 miliar rupiah	3 miliar rupiah s/d 30 miliar rupiah	Kurang dari 3 miliar
2	Total anggaran operasional tahun berjalan yang dialokasikan	Lebih dari 10 miliar rupiah	1 miliar rupiah s/d 10 miliar rupiah	Kurang dari 1 miliar
3	Memiliki kewajiban kepatuhan terhadap peraturan atau standar tertentu	Peraturan atau standar nasional dan internasional	Peraturan dan standar nasional, a.l : UU ITE; Perkominfo No. 4 Tahun 2016; Perkominfo PDP; POJK No. 77; PP PSTE.	Tidak ada peraturan khusus
4	Menggunakan algoritma khusus untuk keamanaan informasi dalam sistem elektronik	Algoritama khusus yang digunakan negara	Algoritma standar public	Tidak ada algoritma khusus
5	Jumlah pemilik akun yang menggunakan sistem elektronik	Lebih dari 5000 pemilik akun	1000 sampai dengan 5000 pemilik akun	Kurang dari 1000 pemilik akun

[41] Dana Moore and John Hebeler, *Peer to Peer : Building Secure, Scalable and Manageable Networks*, (California : The McGraw-Hill Companies, 2002), hlm. 27.

6	Data pribadi yang dikelola sistem elektronik	Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya	Data pribadi yang bersifat individu dan/atau Data Pribadi yang terkait dengan kepemilikan badan usaha	Tidak ada Data Pribadi
7	Tingkat kekritisan data yang ada dalam sistem elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi.	Sangat rahasia	Rahasia dan/atau terbatas	Biasa
8	Tingkat kekritisan proses yang ada dalam sistem elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada pelayanan public	Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung	Proses yang tidak berdampak bagi kepentingan orang banyak
9	Dampak dari kegagalan sistem elektronik	Tidak tersedianya pelayanan publik berskala nasional atau membahayakan keamanan negara	Tidak tersedianya pelayanan publik dalam 1 provinsi.	Tidak tersedianya pelayanan publik dalam 1 kota atau lebih
10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem elektronik (sabotase, terorisme)	Menimbulkan korban jiwa	Terbatas pada kerugian finansial	Mengakibatkan gangguan operasional sementara
Ketentuan Penilaian				
Kategori Sistem Elektronik		Strategis	Tinggi	Rendah
Total Bobot Nilai		36-50	16-35	10-15

Kesesuaian Penyelenggara *P2P Lending* dengan tabel di atas, penulis tandai dengan *shading* warna jingga, namun untuk tabel nomor 9 tidak penulis tandai karena tidak relevan dengan *P2P Lending*. Hasil penjumlahan di atas didapatkan total bobot nilai 20, sehingga dapat disimpulkan bahwa Penyelenggara *P2P Lending* termasuk ke dalam kategori Penyelenggara Sistem Elektronik tingkat tinggi. Konsekuensinya adalah penyelanggara

wajib memenuhi prinsip-prinsip perlindungan Data Pribadi dalam praktik bisnisnya dan menggunakan pendekatan teknologi (salah satunya penerapan ISO/IEC 27001) dalam rangka menjaga kerahasiaan dan keamanan Data Pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi. Terlebih lagi, demi menjaga keamanan, Data Pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia[42]. Hal itu demi kepentingan Pengguna Aplikasi selaku pemilik Data Pribadi yang mempunyai Hak Kebendaan terhadap datanya yang telah disimpan dan diproses dalam bentuk digital (*byte base*) oleh Penyelenggara *P2P Lendin*g.

Jika terjadi kegagalan keamanan pada sistem elektronik Penyelenggara, terdapat kewajiban yang harus dilaksanakan oleh Penyelenggara, salah satunya memberikan pemberitahuan kepada Pengguna selaku pemilik Data Pribadi. Adanya kegagalan pada sistem elektronik Penyelenggara berpotensi mengakibatkan kegagalan perlindungan Data Pribadi (contohnya pada kasus Tokopedia). Terhadap potensi kegagalan dalam perlindungan Data Pribadi, Penyelenggara *P2P Lending* wajib ikut serta dalam pengelolaan celah keamanan teknologi informasi dalam mendukung keamanan informasi di dalam industri jasa keuangan berbasis teknologi informasi. Penyelenggara *P2P Lending* wajib menyediakan sumber daya manusia (SDM) yang mempunyai kemampuan mumpuni di bidang teknologi informasi. Hal ini sebagaimana ketentuan Pasal 14 ayat (1) POJK No. 77 yang mengatur bahwa "penyelenggara wajib menyediakan sumber daya manusia yang memiliki keahlian dan/atau latar belakang di bidang teknologi informasi". SDM di bidang teknologi informasi ini bertanggungjawab jika terjadi kegagalan perlindungan data. Selain itu, sebagai pihak yang menyimpan Data Pribadi, Penyelenggara *P2P Lending* harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran (*data leakage*) atau mencegah setiap kegiatan pemrosesan atau pemanfaatan data pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi tersebut, hal ini sebagaimana ketentuan Pasal 59 ayat (2) huruf (g) PP PMSE.

Jika terjadi kegagalan dalam perlindungan Data Pribadi, Penyelenggara *P2P Lending* wajib memberitahukan secara tertulis kepada pemilik Data Pribadi[43].

---

[42] Indonesia, *Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik*, PP No. 80 Tahun 2019, Ps. 59 ayat (2) huruf (h).

[43] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 26 huruf (e).

Pemberitahuan tersebut disampaikan dengan itikad baik dan dalam bahasa sederhana yang mudah dimengerti oleh pemilik data. PP PSTE mengatur Penyelenggara Sistem Elektronik wajib memberikan pemberitahuan secara tertulis kepada pemilik Data Pribadi mengenai tujuan pengumpulan, aktifitas pemrosesan dan kegagalan perlindungan Data Pribadi. Meskipun PP PSTE dan POJK No. 77 tidak mengatur detail isi pemberitahuan jika terjadi kegagalan perlindungan Data Pribadi seperti layaknya *EU Directive* 95/46 dan GDRP, namun dalam Perkominfo PDP telah terdapat pengaturan mengenai detail isi pemberitahuan tersebut, yaitu[44] :

a. harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi;
b. dapat dilakukan secara elektronik jika pemilik Data Pribadi telah memberikan persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya;
c. harus dipastikan telah diterima oleh pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan
d. pemberitahuan tertulis dikirimkan kepada pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut.

Penyelenggara *P2P Lending* terikat kewajiban untuk memenuhi isi pemberitahuan sebagaimana diatur dalam Perkomindo PDP di atas. Selain isi pemberitahuan tersebut, Penyelenggara *P2P Lending* wajib menyediakan narahubung (*contact person*) dan/atau surat elektronik (*email*) yang mudah dihubungi oleh pemilik Data Pribadi terkait pengelolaan datanya, termasuk *contact person* jika terjadi kegagalan perlindungan data, hal ini untuk memastikan kelangsungan nasabah. Perlu menjadi catatan bahwa ketentuan mengenai jangka waktu pemberitahuan kepada pemilik Data Pribadi jika terjadi kegagalan perlindungan data sebagaimana diatur dalam Perkominfo PDP, yaitu 14 (empat belas) hari sejak diketahuinya kegagalan tersebut[45]. Jangka waktu ini lebih lama dibandingkan ketentuan dalam GDPR yang memberi jangka waktu hanya 72 jam (3 hari) sejak diketahui adanya kegagalan perlindungan data.

B. Pengaturan Akses Data Pribadi dalam *P2P Lending* di Indonesia

Akses Data Pribadi meliputi dua hal, yaitu hak pemilik Data Pribadi untuk mengakses datanya yang tersimpan dan diproses dalam sistem elektronik dan hak pemilik Data

[44] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronik,* Perkominfo No. 20 Tahun 2016, Ps. 28 huruf (c).
[45] *Ibid.*

Pribadi untuk mendapatkan perlindungan hukum dari pengaksesan dan pengungkapan yang tidak sah atas datanya. Akses data berkaitan erat dengan diberikannya informasi mengenai data yang diproses berikut kesempatan untuk melakukan koreksi atas data yang kurang akurat maupun melengkapi data yang kurang lengkap. Tanpa adanya akses, tidak mungkin pemilik Data Pribadi dapat melakukan koreksi atas datanya yang tidak akurat dan/atau kurang lengkap, sehingga hubungan antara akses dan koreksi sangatlah erat. *The Right of Access effectively appears alogical path to rectification*[46]. Akses terhadap pemrosesan data merupakan salah satu hal krusial yang memegang peranan penting dalam transparansi data. *The right of access can play a crucial role in safeguarding fairness, accountability, and responsibility*[47]. Hak untuk mengakses dan mengkoreksi data ini sering diabaikan dan dianggap tidak begitu penting, baik oleh Penyelenggara Sistem Elektronik maupun pemilik Data Pribadi itu sendiri.

Hak pemilik Data Pribadi untuk melakukan akses dan koreksi data harus diimbangi oleh mekanisme yang jelas dan terukur untuk melakukan akses dan koreksi tersebut, misalnya harus didahului dengan permintaan dari pemilik Data Pribadi dan dalam jangka waktu berapa lama akses dan koreksi tersebut wajib dipenuhi oleh Penyelenggara Sistem Elektronik. Selanjutnya, apakah ada atau tidak fitur khusus yang disediakan untuk melakukan akses dan koreksi data. Akses dan koreksi ini merupakan salah satu bentuk kontrol yang dimiliki pemilik Data Pribadi atas datanya yang diproses dan disimpan dalam sistem elektronik.

Kontrol terhadap akses data merupakan dasar bagi terciptanya kondisi transparansi (keterbukaan) dalam pemrosesan data. Kontrol ini meliputi dua sisi, pertama, dari sisi pemilik Data Pribadi mempunyai akses guna mendapatkan informasi yang berhubungan dengean pemrosesan data berikut kesempatan untuk melakukan koreksi data. Kedua, dari sisi Penyelenggara Sistem Ektronik mempunyai kontrol agar data tidak diakses oleh pihak-pihak yang tidak berkepentingan, sehingga Data Pribadi tersebut terlindungi dari pengaksesan dan pengungkapan yang tidak sah. *The notion of control was divided along three dimensions that debate on data protection : control over data access, control over data uses and control through governance*[48]. Dalam pemrosesan data, Penyelenggara Sistem Elektronik harus menentukan siapa saja pekerjanya (karyawan internal perusahaan) yang mempunyai hak untuk mengakses data dalam rangka melakukan pemrosesan data sesuai

[46] Jef Ausloos dan Pierre Dewitte, "Shattering One Way Mirrors - Data Subject Access Rights In Practice", *International Data Privacy Law* Vol. 8 No. 1 (2018), hlm. 8.

[47] *Ibid*, hlm. 4.

[48] Dijana Peras, "Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses", *29th CECIIS* (19-21September 2018), hlm. 113.

dengan tujuan pengumpulan data yang disepakati dengan pemilik Data Pribadi. Penyelenggara Sistem Elektronik harus dapat mengontrol agar data tidak diakses oleh orang-orang (bahkan oleh pekerjanya sendiri) yang tidak berkepentingan. Berkaitan dengan kontrol terhadap pemrosesan data, Vayena dan Blassime berpendapat bahwa :

> *Control over data uses determinates who has the right to access personal data and the purposes for which personal data is used, and decides on the relevance of the purpose and its compliance with the interests and expectations of the data subject. Control over data uses is responsible for keeping unauthorized persons away from the personal data. If the person who tries to access personal data is not authorized to execute specific task, he will not be allowed to do it. Furthermore, it can limit the access of applications in case their request for accessing certain personal data is denied*[49].

EU Directive 95/46 menjamin hak setiap subyek data (pemilik Data Pribadi) untuk mendapatkan informasi dari *Data Controller* mengenai apakah data tersebut sedang diproses atau tidak. Informasi lainnya yang berhak didapatkan oleh pemilik data adalah mengenai tujuan pemrosesan data, kategori data dan siapa saja pihak-pihak yang menerima data dari *Data Controller*. Seluruh informasi tersebut harus dapat diakses oleh pemilik data dan dikomunikasikan menggunakan bahasa yang mudah dimengerti oleh pemilik data[50]. Pemilik Data Pribadi berhak melakukan koreksi data, penghapusan data atau larangan memproses data dalam hal terdapat data yang kurang lengkap dan/atau tidak akurat[51]. Dalam hal *Data Controller* memberikan data tersebut kepada pihak ketiga, maka setiap ada koreksi atas data tersebut, pemilik data berhak mendapatkan pemberitahuan dari *Data Controller* bahwa pihak ketiga tersebut telah melakukan koresi data, sehingga untuk selanjutnya data yang diproses adalah data yang sudah *update* (terkini).

Keterkaitan antara akses data dan informasi ini dapat ditemukan dalam GDPR, dalam *section 2* mereka mengaturnya sebagai *information and access to personal data*. Dalam hal Data Pribadi yang berkaitan dengan pemilik data dikumpulkan, *Data Controller* wajib memberikan dan menyediakan seluruh informasi berkaitan dengan pemrosesan data tersebut kepada pemilik Data Pribadi[52]. Informasi yang disediakan harus dapat diakses dengan mudah oleh pemilik data, antara lain berupa identitas dan kontak *Data Controller* berikut perwakilannya yang sah serta kontak *customer service* yang dapat dengan mudah dihubungi oleh pemilik data dan tujuan pemrosesan data. Bahkan, dalam hal Data Pribadi

---

[49] Vayena, Effy, dan Alessandro Blasimme, "Biomedical Big Data: New Models of Control Over Access, Use and Governance", *Journal of Bioethical Inquiry*, Vo. 14 No. 4 (2017), hlm 501–513 dalam Dijana Peras, "*Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses*", hlm. 118.

[50] *EU Directive* 95/46, Ps. 12.

[51] *Ibid.*

[52] GDPR, Ps. 13 ayat (1).

tersebut hendak dan/atau telah ditransfer ke negara lain, informasi tersebut harus tersedia dan wajib mendapatkan persetujuan terlebih dahulu dari pemilik data. Untuk memastikan adanya keadilan dan transparansi dalam pemrosesan data, *Data Controller* harus menyediakan infromasi, antara lain mengenai berapa jangka waktu data disimpan, adanya akses oleh pemiliknya untuk melakukan koreksi atas data yang salah dan meminta penghapusan datanya serta hak untuk menarik persetujuannya terhadap pemrosesan data kapan saja dikehendaki oleh pemilik data[53].

Bersesuaian dengan *EU Directive* 95/46, GDPR mengatur bahwa pemilik Data Pribadi memilik hak untuk mendapatkan konfirmasi dari *Data Controller* mengenai apakah data tersebut sedang diproses atau tidak, intinya harus ada transparansi dalam pemrosesan data yang dibuktikan dengan adanya kemudahan akses data oleh pemilik data. *The right of access is to be regarded in connection with the principle of transparency, In order to be able to verify the lawfulness of the processing and the accuracy of the data, the subject needs to be able to know whether personal data about him is being processed by the controller or not and if yes, to have access*[54]. Pemilik Data Pribadi berhak untuk mengakses data dan mendapat informasi, antara lain tujuan pemrosesan data, jangka waktu penyimpanan data, kategori data yang diproses, penerima data atau kategori penerima data yang sedang atau akan memproses data tersebut dari *Data Controller* termasuk juga dalam hal data tersebut sedang atau akan diproses oleh negara lain atau organisasi internasional. Informasi lainnya yang harus dapat diakses dengan mudah meliputi informasi untuk melakukan koreksi data, meminta penghapusan data atau melarang memproses data, informasi untuk mengajukan pengaduan ke otoritas pengawas dan informasi mengenai keputusan otomatis (*automated individual decision making*) termasuk informasi mengenai *profiling*[55]. Pasal 16 GDPR mengatur bahwa pemilik Data Pribadi mempunyai hak untuk melakukan koreksi terhadap data yang kurang akurat dan/atau melengkapi data yang tidak lengkap berkaitan dengan pemilik data tersebut, termasuk menyediakan dan/atau memberikan pernyataan tambahan. Permintaan untuk melakukan koreksi tersebut harus dilaksanakan *Data Controller* tanpa penundaan berlarut (*without undue delay*).

Penyelenggaraan transaksi elektronik menurut UU ITE dapat dilakukan dalam lingkup publik dan privat dan para pihak yang melaksanaan transaksi elektronik wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran informasi elektronik

[53] GDPR, Ps. 13 ayat (2).

[54] Andra Giurgiu dan Gérard Lommel, "A New Approach to EU Data Protection : More Control over Personal Data and Increased Responsibility", *Critical Quarterly for Legislation and Law* Vol. 97 No. 1 (2014), hlm. 17.

[55] GDPR, Ps. 15 ayat (1).

dan/atau dokumen elektronik selama transaksi berlangsung[56]. Penyelenggara *P2P Lending* merupakan pihak yang menyelenggarakan transaksi elektronik dalam lingkup privat, sehingga sesuai ketentuan UU ITE, penyelenggara tersebut wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran informasi. Hak untuk mengakses dan melakukan koreksi Data Pribadi secara spesifik tidak dapat ditemukan dalam UU ITE, namun terdapat satu pasal yang menjadi payung hukum bagi PP PSTE untuk mengatur lebih lanjut penyelenggaraan transaksi elektronik, dimana di dalamnya termasuk juga mengatur akses dan koreksi data. Pasal 17 ayat (3) UU ITE mengatur bahwa ketentuan lebih lanjut mengenai penyelenggaraan transaksi elektronik diatur lebih lanjut dengan peraturan pemerintah, ini artinya hal-hal yang bersifat teknis seperti akses dan koreksi data harus dilihat dalam PP PSTE.

Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan[57]. Penyelenggara *P2P Lending* sebagai Penyelenggara Sistem Elektronik berdasarkan PP PSTE wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum, salah satunya dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut. Kemudahan pemilik Data Pribadi mengakses informasi terhadap pemrosesan data berkontribusi terhadap tercapainya pemenuhan privasi, begitu pula sebaliknya, hambatan pemilik Data Pribadi mengakses informasi mengenai pemrosesan datanya berkontribusi terhadap gangguan privasi. *Unequal access to information may contribute to unequal access to privacy*[58]. Prinsip-prinsip perlindungan Data Pribadi wajib dilaksanakan dengan baik oleh Penyelenggara *P2P Lending*, termasuk pemrosesan data dilakukan dengan melindungi keamanan data dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan data. *All organisations are required to protect personal data in their possession or control by "making reasonable security arrangements" to prevent unauthorized access*[59]. Selain mencegah terjadinya pengungkapan tidak sah, Penyelenggara *P2P Lending* juga wajib mencegah agar jangan sampai terjadi pengaksesan yang tidak sah dari pihak lain (di luar Penyelenggara) yang tidak berkepentingan.

---

[56] Indonesia, *Undang-Undang Informasi dan Transaksi Elektronik,* UU No. 11 Tahun 2008, LN No. 58 Tahun 2008, Ps. 17 ayat (1).

[57] Indonesia, *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP No. 71 Tahun 2019, Ps. 1 angka (15).

[58] Stacy Ann Elvy, "Paying For Privacy And The Personal Data Economy", *Columbia Law Review* Vol. 117 No. 6 (Oktober 2017), hlm. 1338.

[59] Simon Chesterman, "After Privacy : The Rise of Facebook, The Fall of Wikileaks, And Singapore's Personal Data Protection Act 2012", *Singapore Journal of Legal Studies* (Desember 2012), hlm. 410.

POJK No. 77 mewajibkan Penyelenggara *P2P Lending* untuk menyediakan akses informasi kepada Penerima Pinjaman selaku pemilik Data Pribadi atas posisi pinjaman yang diterima[60]. Kapanpun pemilik data meminta informasi tersebut, Penyelenggara wajib menyediakan akses untuk itu. *Right to access can be exercised at any time of a personal data processing*[61]. Dalam rangka akses data, Penyelenggara *P2P Lending* wajib memastikan tersedianya proses autentikasi, verifikasi, dan validasi yang mendukung kenirsangkalan dalam mengakses Data Pribadi.

Ruang lingkup informasi berdasarkan POJK hanya satu saja, yaitu posisi pinjaman yang diterima (data keuangan), namun di luar informasi tersebut Penerima Pinjaman tetap bisa mengakses informasi lainnya. Hal ini dikarenakan kegitan *P2P Lending* termasuk dalam kegiatan transaksi elektronik dan terikat dengan PP PSTE, sehingga informasi yang berhak diakses oleh Penerima Pinjaman tidak hanya informasi yang diatur dalam POJK saja, akan tetapi juga meliputi informasi yang diatur dalam PP PSTE. Dengan demikian, informasi identitas Penyelenggara *P2P Lending* berikut tanda berizin/terdaftar di OJK wajid diberikan akses kepada pemilik Data Pribadi. Selain itu, informasi mengenai layanan dan/atau produk dari Penyelenggara *P2P Lending* wajib disampaikan secara akurat, jujur, jelas, dan tidak menyesatkan serta dituangkan dalam dokumen atau sarana lain yang dapat digunakan sebagai alat bukti.

Sebagaimana disebutkan di atas, akses data meliputi juga hak pemilik Data Pribadi untuk mendapat perlindungan dari pengaksesan data yang tidak sah, untuk menjamin hak tersebut, ada dua hal yang harus diperhatikan, pertama, Penyelenggara *P2P Lending* wajib membuat suatu sistem elektronik melalui *Privacy by Design* untuk menjamin *data security*. Kedua, Penyelenggara *P2P Lending* dilarang dengan cara apapun memberikan data dan/atau informasi maupun memberi kesempatan untuk dapat diakses Data Pribadi kepada pihak ketiga yang tidak mempunyai *legitimate interest*, kecuali atas persetujuan pemilik Data. *The operator is prohibited by any means to provide data and/or information concerning users to third-parties except where consent is given*[62].

Mengacu pada *Right of Access* dalam *EU Directive* 95/46 dan GDPR, jika Data Pribadi Penerima Pinjaman dikirim ke pihak ketiga (misalnya perusahaan jasa penagihan pinjaman gagal bayar), informasi mengenai identitas pihak ketiga tersebut wajib disediakan

---

[60] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 20 ayat (3).

[61] Gianclaudio Malgieri dan Giovanni Comande, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* Vol. 7 No. 4 (2017), hlm. 247.

[62] Kevin Davis, Rodney Maddock dan Martin Foo, "Catching up with Indonesia's Fintech Industry", *Law and Financial Markets Review* Vol. 11 No. 1 (2017), hlm. 38.

oleh Penyelenggara *P2P Lending* dan dikomunikasikan kepada Penerima Pinjaman dengan bahasa yang sederhana dan mudah dipahami. OJK dalam kertas kerja untuk tahap perizinan *P2P Lending* mensyaratkan bahwa identitas pihak ketiga yang menerima Data Pribadi dari Penyelenggara *P2P Lending* wajib diinformasikan kepada pemilik Data Pribadi dan sebelum diberikan dan/atau ditransfer kepada pihak ketiga, Penyelenggara *P2P Lending* wajib meminta persetujuan terlebih dahulu dari pemilik Data Pribadi. Hal ini untuk memastikan bahwa hanya perusahaan yang ditunjuk oleh Penyelenggara *P2P Lending* saja yang bisa melakukan penagihan pinjaman gagal bayar terhadap Penerima Pinjaman. Selain itu, informasi lain yang wajib disediakan adalah informasi mengenai obyek yang ditransaksikan, kelaikan atau keamanan sistem elektronik, tata cara penggunaan perangkat, syarat kontrak, prosedur mencapai kesepakatan, jaminan privasi dan/atau perlindungan Data Pribadi dan nomor telepon pusat pengaduan[63]. Berbagai informasi yang wajib disediakan Penyelenggara *P2P Lending* sebagaimana diatur dalam PP PSTE ini kurang lebih sama pengaturannya dengan GDPR dan *EU Directive* 95/46. Tidak semua informasi dapat diakses oleh Penerima Pinjaman, terdapat pembatasan informasi yang tidak dapat diakses, yaitu informasi terkait identitas Pemberi Pinjaman[64], hal ini merupakan konsekuensi logis dari suatu hak yang selalu mempunyai batasan-batasan tertentu. *An individual has a limited right to request access to personal data and request the correction of errors or omissions in personal data concerning him or her*[65].

Pemilik data berhak melakukan koreksi atas data yang tidak akurat dalam artian memutakhirkan Data Pribadinya (melakukan *update* data) atau melengkapi datanya yang kurang lengkap. Hak tersebut bahkan oleh PP PSTE dimplementasikan dengan memberi kewajiban Penyelenggara Sistem Elektronik menyediakan fitur berupa fasilitas untuk melakukan koreksi data[66]. Perkominfo PDP juga memberikan hak kepada pemilik data untuk kemudahan akses dan koreksi data (informasi elektronik dan/atau dokumen elektronik)[67]. Hak untuk melakukan koreksi data wajib diberikan sebagai kesempatan kepada pemilik Data Pribadi untuk mengubah atau memperbarui data tanpa menganggu sistem pengelolaan Data Pribadi. Kesempatan tersebut meliputi kesempatan untuk

[63] Indonesia, *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP No. 71 Tahun 2019, Ps. 29.

[64] Indonesia, *Peraturan Otoritas Jasa Keuangan Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*, POJK No. 77 Tahun 2016, Ps. 20 ayat (4).

[65] Simon Chesterman, "After Privacy : The Rise of Facebook, The Fall of Wikileaks, And Singapore's Personal Data Protection Act 2012", hlm. 410.

[66] Indonesia, *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP No. 71 Tahun 2019, Ps. 30 ayat (2) huruf (a).

[67] Indonesia, *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronik,* Perkominfo No. 20 Tahun 2016, Ps. 2 ayat (2) huruf (i).

memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik. PP PMSE mengatur juga masalah koreksi data ini, Pasal 59 ayat (2) huruf (d) mengatur bahwa Data Pribadi harus akurat dan harus selalu *up to date* dengan memberikan kesempatan kepada pemilik data untuk memutakhirkan data pribadinya. Kesempatan pemutakhiran data tersebut merupakan bagian dari standar perlindungan Data Pribadi atau kelaziman praktik bisnis yang berkembang.

Baik UU ITE, Perkominfo PDP, PP PSTE, dan POJK No. 77 semuanya telah mengatur hak pemilik Data Pribadi untuk melakukan akses dan koreksi, namun tidak ada satu pasal pun dalam peraturan perundang-undangan tersebut yang mewajibkan Penyelenggara Sistem Elektronik membuat mekanisme khusus untuk melakukan akses dan koreksi. PP PSTE hanya mewajibkan adanya fitur (bukan mekanisme) untuk melakukan koreksi data, lalu bagaimana dalam hal terdapat Penyelenggara *P2P Lending* yang dalam aplikasinya belum atau tidak mempunyai fitur untuk melakukan akses dan koreksi, ini menjadi persoalan tersendiri. Jadi, dalam tataran hukum positif di Indonesia memang sudah diatur dan diakomodir hak untuk melakukan akses dan koreksi data, namun penerapannya secara teknis di bidang *P2P Lending*, hampir semua Penyelenggara belum atau tidak menyediakan fitur khusus dalam aplikasinya untuk mengakses dan melakukan koreksi data. *Modalities should be provided for facilitating the exercise of the data subject's rights, including mechanisms to request access to and rectification or erasure of personal data*[68]. Seharusnya ada pasal khusus dalam PP PSTE yang mengatur mekanisme (tidak hanya fitur) untuk melakukan akses dan koreksi, seperti halnya mekanisme penghapusan informasi elektronik dan/atau elektronik yang tidak lagi relevan (*Right to Erasue* dan *Right to Delisting*).

RUU PDP mengatur masalah akses dan koreksi data, pemilik Data Pribadi berhak mengakses Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan. Tidak hanya hak untuk mendapatkan akses, namun pemilik data juga memiliki hak untuk mendapat perlindungan hukum terkait keamanan Data Pribadi dari pengaksesan dan pengungkapan yang tidak sah. Setiap pihak yang tidak mempunyai *legitimate interest* tidak diperbolehkan melakukan akses data, Pengendali Data Pribadi (istilah yang digunakan dalam RUU PDP) wajib mencegah Data Pribadi diakses secara tidak sah. Pemilik Data Pribadi berhak untuk mengakses informasi mengenai legalitas dari pemrosesan data, tujuan pemrosesan data, jenis dan relevansi Data Pribadi yang akan

[68] Dijana Peras, "Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses", hlm. 116.

diproses, periode retensi dokumen yang memuat Data Pribadi, rincian mengenai informasi yang dikumpulkan dan jangka waktu pemrosesan Data Pribadi[69].

Akses diberikan kepada pemilik Data Pribadi terhadap data yang diproses beserta rekam jejak pemrosesan data sesuai dengan jangka waktu penyimpanan Data Pribadi[70]. Pemberian akses data wajib dilakukan dalam jangka waktu paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan akses dari pemilik data[71]. RUU PDP memberikan pembatasan akses perubahan terhadap Data Pribadi kepada Pemilik Data Pribadi dalam hal diketahui atau sepatutnya diduga membahayakan keamanan atau kesehatan fisik atau kesehatan mental Pemilik Data Pribadi dan/atau orang lain, berdampak pada pengungkapan Data Pribadi milik orang lain dan/atau bertentangan dengan kepentingan pertahanan dan keamanan nasional.

IV. KESIMPULAN

Penyelenggara *P2P Lending* merupakan Penyelenggara Sistem Elektronik tingkat tinggi karena; pertama, Penyelenggara *P2P Lending* diwajibkan mendapat Sertifikasi ISO/IEC 27001 dan kedua, sistem elektronik Penyelenggara *P2P Lending* merupakan sistem elektronik yang berdampak pada kepentingan sektor tertentu, yaitu sektor keuangan. Konsekuensi dari dua hal tersebut, maka Data Pribadi yang diperoleh oleh Penyelenggara wajib dijaga keamanannya dan dilakukan langkah-langkah manajemen pengamanan informasi melalui standar ISO/IEC 27001. Penerapan standar ISO/IEC 27001 ini untuk memastikan tercapainya Keamanan Data Pribadi, yaitu terjaganya Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*). Keamanan.

UU ITE, Perkominfo PDP, PP PSTE, dan POJK No. 77 serta RUU PDP semuanya telah mengatur hak Pemilik Data Pribadi untuk melakukan Akses. Penerima Pinjaman selaku Pemilik Data Pribadi berhak mengakses Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan. Tidak hanya hak untuk mendapatkan akses, namun Penerima Pinjaman juga memiliki hak untuk mendapat perlindungan hukum dari pengaksesan dan pengungkapan yang tidak sah atas Data Pribadinya. Setiap pihak yang tidak mempunyai *legitimate interest* tidak diperbolehkan melakukan akses Data Pribadi Penerima Pinjaman.

[69] RUU PDP, Ps. 24 ayat (1).
[70] RUU PDP, Ps. 32 ayat (1).
[71] *Ibid*, Ps. 32 ayat (2).

V. SARAN

Penyelenggara *P2P Lending* wajib menerapkan sistem manajemen pengamanan informasi, baik melalui pendekatan peraturan perundang-undangan maupun melalui pendekatan teknologi informasi, untuk menciptakan praktik bisnis yang melindungi keamanan Data Pribadi Penerima Pinjaman, baik karena adanya kerentanan kebocoran Data Pribadi maupun adanya kerentanan pengaksesan secara tidak sah dari pihak lain yang tidak mempunyai *legitimate interest*. Di sisi lain, Pemerintah melalui OJK dan Kominfo selaku regulator dan pengawas wajib menerapkan sanksi hukum tegas terhadap setiap Penyelenggara *P2P Lending* yang tidak menerapkan Keamanan Data Pribadi dalam menjalankan praktik bisnisnya. Selain itu, Penerapan standar ISO/IEC 27001 wajib dilakukan Penyelenggara *P2P Lending* dan pelaksanaannya diawasi dengan ketat oleh OJK bersama-sama dengan Kominfo maupun asosiasi sektoral, yaitu Asosiasi Pendanaaan Bersama *Fintech* Indonesia (AFPI).

OJK wajib memastikan bahwa akses Penerima Pinjaman terhadap Data Pribadinya dapat mudah dilakukan, baik melalui fitur yang disediakan Penyelenggara *P2P Lending* maupun melalui permintaan *by email* harus ada sebagai sarana agar Penerima Pinjaman masih memiliki kontrol atas Data Pribadinya. Hal ini wajib menjadi perhatian OJK saat melakukan penilaian terhadap Penyelenggara *P2P Lending* di tahap pemberian perizinan mengenai adanya jaminan Akses Data Pribadi oleh Penerima Pinjaman, baik meliputi status pinjamannya maupun terkait pemrosesan Data Pribadi.

DAFTAR PUSTAKA

Buku

Adams, James and Kletter, Richard. *Artificial Intelligence : Confronting The Revolution*. Middletown : Endeavour Media Ltd., 2018.

Djafar, Wahyudi, Sunigar, Bernhard Ruben Fritz dan Setianti, Blandina Lintang. *Perlindungan Data Pribadi : Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusi*. Jakarta : Lembaga Studi dan Advokasi Masyarakat/ELSAM, 2016.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta : Prenadamedia Group, 2014.

Moore, Dana and Hebeler, John. *Peer to Peer : Building Secure, Scalable and Manageable Networks*. California : The McGraw-Hill Companies, 2002.

Prodjodikoro, Wirjono. *Azas-azas Hukum Perjanjian*. Bandung : Sumur, 1993.

Rosadi, Sinta Dewi. *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. Bandung : PT Refika Aditama, 2015.

Soekanto, Soerjono dan Mamudji, Sri. *Penelitian Hukum Normatif*. Cet ke-8. Jakarta : PT Raja Grafindo Persada, 2004.

Subekti. *Pokok-Pokok Hukum Perdata*. Jakarta : Intermasa, 1979.

Wiradipradja, E.Saefullah. *Penuntun Praktis Metode Penelitian dan Penelitian Karya Ilmiah*. Cet. 2. Bandung : CV Keni Media, 2016.

Jurnal

Ausloos, Jef dan Dewitte, Pierre. "*Shattering One Way Mirrors - Data Subject Access Rights In Practice*". *International Data Privacy Law,* Vol. 8 No. 1, 2018, 4-28 : 8.

Chesterman, Simon. "*After Privacy : The Rise of Facebook, The Fall of Wikileaks, And Singapore's Personal Data Protection Act 2012*". *Singapore Journal of Legal Studies*, 2012, 391-415 : 410.

Davis, Kevin, Maddock, Rodney dan Foo, Martin, "*Catching up with Indonesia's Fintech Industry*". *Law and Financial Markets Review*, Vol. 11 No. 1, 2017, 33-40 : 38.

Elvy, Stacy Ann. "*Paying For Privacy And The Personal Data Economy*". *Columbia Law Review*, Vol. 117 No. 6, 2017, 1369-1459 : 1338.

Giurgiu, Andra dan Lommel, Gérard. "*A New Approach to EU Data Protection : More Control over Personal Data and Increased Responsibility*". *Critical Quarterly for Legislation and Law*, Vol. 97 No. 1, 2014, 10-27 : 17.

Hirsch, Dennis D. "T*he Glass House Effect: Big Data, The New Oil, and the Power of Analogy*". *Maine Law Review* Vol. 66 No. 2, 2014, 374-395 : 374.

Higashizawa, Noriko dan Aihara, Yuri. "*Data Privacy Protection of Personal Information Versus Usage of Big Data : Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)*". *Defense Counsil Journal*, Vol. 84 No. 4, 2017, 1-15 : 1.

Jankovic, Dejan Z. "*Key Security Measures For Personal Data Protection In IT Systems". 20th Telecomunication Forum, TELFOR 2012*, 2012, 79-82 : 79.

Kuner, Christopher, *et al*.. "*The Rise Of Cybersecurity And Its Impact On Data Protection*". *International Data Privacy Law*, Vol. 7 No. 2, 2017, 73-75 : 73.

Latumahina, Rosalinda Elsina. "*Aspek Hukum Perlindungan Data Pribadi di Dunia Maya". Jurnal Gema Aktualita*, Vol. 3 No. 2, 2014, 14-25 : 14.

Loi, Michele dan Dehaye, Paul Olivier. "*If Data Is The New Oil, When Is The Extraction of Value From Data Unjust*". *Philosophy and Public Issues – Tyranny, Democracy, and Economy*, Vol. 7 No. 2, 2017, 137-178 : 139.

Malgieri, Gianclaudio dan Comande, Giovanni. "*Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*". *International Data Privacy Law*, Vol. 7 No. 4, 2017, 243-265 : 247.

Peras, Dijana. "*Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses*", *29th CECIIS,* 2018, 113-121 : 113.

Rosadi, Sinta Dewi. "*Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia". Jurnal Veritas et Justicia*, Vol. 4 No. 1, 2018, 88-110 : 88.

Indonesia, Undang-Undang Dasar 1945 Amandemen II, Pasal 28 Huruf (G) Ayat (1).

Indonesia, Undang-Undang No. 21 Tahun 2011 Tentang Otoritas Jasa Keuangan, Lembaran Negara Republik Indonesia (LNRI) Nomor 111 Tahun 2011, dan Tambahan Lembaran Negara (TLN) Nomor 5253.

Indonesia, Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, Lembaran Negara Republik Indonesia (LNRI) Nomor 251 Tahun 2016, dan Tambahan Lembaran Negara (TLN) Nomor 5952.

Indonesia, Peraturan Otoritas Jasa Keuangan No. 77 Tahun 2016 Tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, Lembaran Negara Republik Indonesia (LNRI) Tahun 2016 Nomor 324, dan Tambahan Lembaran Negara (TLN) Nomor 600.

Indonesia, Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Berita Negara Republik Indonesia (BNRI) Tahun 2016 Nomor 1829.

Indonesia, Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi.

Indonesia, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara Republik Indonesia (LNRI) Tahun 2016 Nomor 185, dan Tambahan Lembaran Negara (TLN) Nomor 6400.

Indonesia, Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, Lembaran Negara Republik Indonesia (LNRI) Tahun 2019 Nomor 222, dan Tambahan Lembaran Negara (TLN) Nomor 6420.

Disertasi

Salam, Abdul. *Hukum Kebendaan Digital (Digital Property) : Kajian Hukum Keperdataan Terhadap Kebendaan Digital*. Ringkasan Disertasi Doktorr Ilmu Hukum Universitas Indonesia, 2017.

Bahan Seminar dan Lain-Lain

Hadad, Muliaman D.. "Financial Technology (Fintech) di Indonesia)". Makalah disampaikan pada Kuliah Umum Tentang *Fintech*, Jakarta, 2 Juni 2017.

Minmin, Fan and Wang, Yang. "*Figuring The Future Of Financial Technology*". China Daily European Edition, (2 December 2016).

Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP).

Surat Otoritas Jasa Keuangan No. S-382/NB.213/2018 tanggal 8 Juni 2018 perihal Tanda Bukti Terdaftar PT Artha Permata Makmur

World Economic Forum dan A.T. Kearney. *Rethinking Personal Data : A New Lens for Strengthening Trust*, 2014.

General Data Regulation Protection/GDPR (European Union Regulation 2016/679).

Internet

Budhijanto, Danrivanto. "*Data As New Oil dalam Konstruksi Hukum Ekonomi Digital di Indonesia*". https://www.hukumonline.com/berita/baca/ diakses 25 November 2019.

Parkins, David. "*The World's Most Valuable Resource Is No Longer Oil, But Data*". https://www.economist.com/leaders/ diakses 25 November 2019.

Pertiwi, Wahyunanda Kusuma."*Sidang Perdana Kasus Kebocoran Data Tokopedia Digelar Hari Ini*", https://tekno.kompas.com/read/2020/06/10/09144017/ diakses 24 Agustus 2020.