ISSN 2828-1098 (Print)
ISSN 2828-075X (Online)

Article

ELIGIBLE Journal of Social Sciences
Volume 2 Number 1 (2023)
https://doi.org/10.53276/eligible.v2i1.66

Perlindungan Data Pribadi Konsumen Pinjaman *Online*: Suatu Analisis

Russel Butarbutar♦, Bernedete Nurmawati

Fakultas Hukum, Universitas Bung Karno

Abstract: This study discusses the protection of consumer personal data Peer to peer Lending. This research was conducted in a normative juridical manner with a comparative law approach and case law. Legal protection of personal data, especially Peer to Peer (P2P) Lending customers in Indonesia, needs to be realized immediately through the ratification of the Government Regulations or/and the Law on Personal Data Protection to guarantee citizens' rights to personal protection and raise public awareness as well as ensure recognition and respect for the importance of personal data protection. The Personal Data Protection Law must regulate data protection accurately and transparently and regulates (1) restrictions on how personal data is collected, stored, or shared; (2) require companies to disclose how they use personal data; (3) mandate a minimum level of personal data protection; (4) legal guarantee of the rights of the owner of personal data; (5) the prohibition on the use of personal data is aimed at people who obtain or collect or disclose or use personal data that does not belong to them to unlawfully benefit themselves or others or may cause losses to the owner of personal data or consumers; (6) formulation of administrative sanctions and criminal sanctions that are just, certain, and legally beneficial and economy.

Key Words: Protection; Data; Personal; Consumers: P2P; Lending

Abstrak: Penelitian ini membahas perlindungan data pribadi konsumen pinjaman online. Penelitian ini dilakukan secara yuridis normatif dengan pendekatan perbandingan hukum dan kasus hukum. Perlindungan hukum tentang data pribadi khususnya nasabah Pinjaman Online di Indonesia perlu untuk segera direalisasikan melalui pengesahan Peraturan Pemerintah dan/atau Undang-Undang tentang Perlindungan Data Pribadi untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Undang-Undang Perlindungan Data Pribadi harus mengatur perlindungan data secara akurat dan transparan serta mengatur tentang (1) pembatasan cara pengumpulan, penyimpanan atau pembagian data pribadi; (2) mewajibkan perusahaan untuk mengungkapkan cara mereka menggunakan data pribadi; (3) mengamanatkan tingkat mimimun perlindungan data pribadi; (4) jaminan hukum terhadap hak pemilik data pribadi; (5) larangan dalam penggunaan data pribadi ditujukan kepada orang yang memperoleh atau mengumpulan atau mengungkapkan atau menggunakan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian pemilik data pribadi atau konsumen; (6) perumusan sanksi administratif dan sanksi pidana yang berkeadilan, berkepastian, dan bermanfaat secara hukum. dan ekonomi.

Kata Kunci: Perlindungan; Data; Pribadi; Konsumen: Pinjaman *Online*

♦**Corresponding author:** Russel Butarbutar, russelbutar@gmail.com, Faculty of Law, Universitas Bung Karno, 10310, Jakarta, Indonesia

PENDAHULUAN

Perlindungan data khususnya perlindungan data pribadi dalam transaski elektronik menjadi semakin penting untuk dibahas dan direalisasikan. Sementara, banyak masyarakat yang belum paham, bahwa data pribadi rawan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab (Pratiwi, 2021).

Melihat sejarah undang-undang perlindungan data dimulai di negara bagian Hesse di Jerman tahun 1970. Kemudian diikuti Swedia pada tahun 1973, Amerika Serikat pada tahun 1974, Inggris pada tahun 1984 (Makarim 2003). Kemudian sampai saat ini, sudah puluhan negara yang memiliki undang-undang perlindungan data (Okezone, 2021). Menurut Litbang MNC Portal, negara ASEAN yang telah punya Undang-Undang Perlindungan Data Pribadi diantaranya: Malaysia, Singapura, Filipina, Thailand. Bahkan negara Asia seperti China telah meratifikasi RUU Perlindungan Data Pribadi melalui Kongres Nasional Rakyat telah mengesahkan UU Perlindungan Data Pribadi pada Jumat (20/8/2021) (Bisnis Indonesia, 2021).

Faktanya saat ini, seiring berkembangnya bisnis digital yang menghadirkan bisnis pinjaman *online* (*financial technology*) yang sering disebut *Fintech* atau Pinjol. Pinjaman *Online* menjadi salah satu produk finansial, yang paling diminati masyarakat Indonesia karena memiliki proses pengajuan yang cepat, syarat mudah dan juga praktis. Hal ini juga mendorong Bank, *Fintech* dan Lembaga Keuangan lainnya untuk menawarkan Pinjaman *Online* cepat cair untuk membantu masyarakat yang membutuhkan. Masyarakat tak perlu lagi mendatangi Bank dengan mengajukan permohonan secara langsung untuk mendapatkan pinjaman, proses peminjaman uang cukup diakses melalui *smartphone*, seperti *Apple Store* (IOS) atau *Google Play Store* (Android) maupun laptop yang terkoneksi dengan internet (Hasela, 2020).

Terlepas dari kemudahan akses pembiayaan dari pinjaman *online*, di sisi lain menghadirkan masalah baru, yaitu seringkali seseorang atau konsumen pinjaman *online* menerima panggilan suara atau pesan singkat dari seseorang yang tidak dikenal, yang berisi kata-kata kasar dan mendiskreditkan seseorang. Artinya data konsumen telah ada pada *database* kontak selular orang dimaksud, dan data itu telah diakses serta digunakan tanpa seizin pemiliknya oleh seseorang atau sekelompok orang yang merupakan *debt collector* dari penyedia jasa pinjaman permodalan secara digital (*online*), yang memberikan layanan *peer to peer* (P2P) *lending* atau pinjaman *online* (*pinjol*) (Dewayani, 2021).

Pinjaman *Online* kian hari terus menjadi sorotan publik. Berbagai kasus pelanggaran lembaga Pinjaman *Online* mulai bermunculan di media massa. Bentuk pelanggaran oleh Pinjaman *Online* ini juga beragam jenisnya. Mulai dari penagihan intimidatif (Pasal 368 KUHP dan Pasal 29 jo 45 UU ITE), penyebaran data pribadi (Pasal 32 jo Pasal 48 UU ITE), penipuan (Pasal 378 KUHP) hingga pelecehan seksual melalui media elektronik (Pasal 27 ayat (1) jo Pasal 45 ayat (1) UU ITE) yang diduga terjadi dalam persoalan ini. Bahkan Pinjaman *Online* ini telah merenggut nyawa nasabah yang memilih bunuh diri akibat depresi karena penagihan pinjaman tersebut. Namun, penyelesaian hukum permasalahan ini masih minim sehingga kasus-kasus serupa terus bermunculan. Peminjam *online* bisa juga disebut sebagai konsumen atau sebagai pemilik data yang harus dilindungi kepentingan hukumnya dalam setiap transaksi jenis apapun.

Berangkat dari penjelasan di atas, penting untuk melakukan penelitan tentang bagaimanakah perlindungan data pribadi konsumen pinjaman *online* seharusnya diatur dalam peraturan perundang-undangan Indonesia. Untuk menjawab pertanyaan tersebut, penelitian ini akan dilakukan dengan beberapa tahapan, yaitu dimulai dari tahapan metode, dilanjutkan dengan pembahasan, dan terakhir disajikan dalam bentuk kesimpulan.

METODE

Metode penelitian yang dipakai dalam penulisan ini adalah metode kualitatif (QuestionPro, 2020) yang dalam riset hukum disebut metode penelitian hukum normatif yang berasal dari kaedah atau norma yang merupakan patokan atau pedoman perilaku manusia yang dianggap pantas (Benuf, Kornelius, 2020), yang dilakukan dengan pendekatan konsep, perbandingan, dan perundang-undangan (Yuwono, Felix, Emanuel Raja Damaitu, 2021) untuk memberikan penjelasan atau deskripsi tentang pertanyaan penelitian.

PEMBAHASAN

Prinsip Dasar Perlindungan Data Pribadi

Perlindungan data pribadi meliputi nama, *e-mail*, nomor telepon genggam merupakan data yang sangat berharga karena dapat nilai ekonomi yang didapatkan dalam dunia bisnis. Hal tersebut dinamakan berkas digital (*digital dossier*) yang merupakan kumpulan informasi data pribadi yang dimiliki oleh sebagian besar bahkan hampir seluruh orang dengan memanfaatkan teknologi internet yang dikembangkan oleh pihak swasta yang sangat berisiko terjadinya pelanggaran hak privasi atas data pribadi seseorang (Priscyllia, 2019).

Dalam pengolahan data, perlu untuk mengetahui pihak-pihak yang biasanya berhubungan dengan perlindungan data pribadi menurut *European Union-Data Protection Directive* (Dataguidance.com, 2022) diantaranya: (1) *Subyek data*, yaitu orang yang data pribadinya di proses; (2) *Controller*, yaitu pribadi kodrati atau pribadi hukum, ottoritas publik, agen, atau lembaga lain yang baik sendiri maupun bersama-sama menentukan tujuan dan cara pemrosesan data pribadi; jika tujuan dan cara pemrosesan data ditentukan oleh negara atau undang-undang, *controller* ditentukan oleh negara atau undang-undang; (3) *Processor*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang memproses data pribadi atas nama *controller*; (4) *Third party*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain di bawah wewenang *controller* atau *processor*, berwenang untuk mengolah data; (5) *Recipient*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang kepadanya data disingkapkan; (6) *Supervisory Authorities*, yaitu badan/lembaga publik yang independen yang bertugas mengawasi perlindungan data pribadi, yang mempunyai wewenang untuk menyelidiki kegiatan pengolahan data, termasuk hak untuk mengakses data tersebut dan wewenang untuk menghalangi pengiriman data ke pihak ketiga. Badan ini harus juga mendengarkan keluhan dari subyek data dan harus mengeluarkan laporan, paling tidak laporan tahunan sesuai dengan undang-undang perlindungan data (Wrigley, 2019).

Menurut Undang-Undang Perlindungan Data Pribadi Uni Eropa, prinsip dasar perlindungan data pribadi yang harus diperhatikan oleh *data controller*, yaitu: (1) data pribadi harus diperoleh secara jujur dan sah; (2) data pribadi harus memiliki hanya untuk satu tujuan atau lebih yang spesifik dan sah, dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan-tujuan tersebut; (3) data pribadi harus layak, relevan, dan tidak terlalu luas dalam hubungannya dengan tujuan-tujuan pengolahannya; (4) data pribadi harus akurat dan *up to date*; (5) data pribadi harus diproses sesuai dengan tujuannya dan tidak boleh dikuasai lebih lama dari waktu yang diperlukan untuk kepentuingan tujuan-tujuan tersebut; (6) data pribadi harus diproses sesuai dengan hak-hak subyek data sebagaimana yang diatur dalam undang-undang; (7) tindakan-tindakan pengamanan yang memadai harus diambil untuk menghadapi kegiatan pemrosesan data pribadi yang sah serta atas kerugian yang tidak terduga atau kerusakaan dari data priabdi; (8) data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Wilayah Ekonomi Eropa kecuali jika negara atau wilayah tersebut menjamin dengan suatu

https://doi.org/10.53276/eligible.v2i1.66

tingkat perlindungan terhadap hak-hak dan kebebasan-kebebasan subyek data sehubungan dengan pemrosesan data pribadi (Dataguidance.com, 2022).

Lebih lanjut tentang prinsip perlindungan data Pribadi dalam Bab 5 GDPR 2018 yang mengedepankan hak individu (pemilik data), yang meliputi (Hutsix, 2021):

(1) *Hak untuk diberitahu*, baik pemroses dan pengontrol data sekarang berkewajiban untuk memberikan informasi kepada subjek data tentang data pribadi yang dikumpulkan, bagaimana data tersebut akan digunakan, dengan siapa akan dibagikan, untuk berapa lama akan disimpan dan tujuan pemrosesannya.
(2) *Hak akses, d*engan permintaan, subjek data individu berhak atas konfirmasi bahwa data mereka sedang diproses, akses ke data tersebut serta informasi lebih lanjut mengenai pengambilan keputusan otomatis, atau periode penyimpanan yang diharapkan.
(3) *Hak untuk memperbaiki*, dengan prinsip yang sesuai dalam 'akurasi', subjek data berhak untuk memperbaiki data pribadi jika tidak akurat atau tidak lengkap.
(4) *Hak untuk menghapus*, juga dikenal sebagai 'hak untuk dilupakan', hak ini memungkinkan subjek data untuk meminta penghapusan atau penghapusan data jika tidak ada alasan kuat untuk melanjutkan pemrosesan atau ketersediaannya. Hak ini dalam beberapa keadaan mungkin juga mewajibkan, misalnya, perusahaan mesin telusur untuk menghapus hasil tertentu, atau membatasi kemampuannya untuk ditemukan.
(5) *Hak untuk membatasi pemrosesan*, pemrosesan adalah operasi apa pun yang dilakukan pada data pribadi. Ini termasuk menggunakan, melihat, mengubah atau menghapus data. Individu dapat memblokir atau menahan pemrosesan data pribadi karena alasan berikut: Data yang tidak akurat, pemrosesan data yang melanggar hukum, atau penolakan yang tertunda untuk memproses data oleh subjek data.
(6) *Hak atas portabilitas data*, mengizinkan individu untuk mendapatkan dan menggunakan kembali data pribadi mereka di berbagai layanan, hak ini berarti data individu harus tersedia dalam format yang dapat dibaca mesin yang umum digunakan, dengan cara yang memungkinkan data tidak dikirim ulang secara terus-menerus.
(7) *Hak untuk menolak*, mengizinkan individu untuk menolak (karena alasan tertentu) pemrosesan data pribadi mereka, serta mewajibkan organisasi untuk memberi tahu individu tentang hak ini pada saat komunikasi pertama.
(8) *Hak terkait dengan pengambilan keputusan dan pembuatan profil otomatis*. Salah satu hak yang lebih terperinci dan teknis yang diberikan berdasarkan GDPR, antara lain, memberikan hak kepada individu untuk memilih keluar dari proses pengambilan keputusan otomatis, keputusan tantangan, dan/atau keputusan otomatis ditinjau oleh manusia.

Pada dasarnya prinsip perlindungan data pribadi harus menghormati privasi, yaitu kebebasan Pemilik Data Pribadi untuk menyatakan rahasia atau tidak menyatakan rahasia data pribadinya, kecuali ditentukan lain sesuai dengan peraturan perundang-undangan. Privasi dibagi menjadi dua jenis, yaitu privasi otonomi, dan privasi informasi. Otonomi privasi adalah hak individu yang bebas dari campur tangan pihak luar. Sementara privasi informasi (*tort*) adalah hak individu untuk menentukan sejauh mana informasi tentang diri mereka disampaikan kepada orang lain, baik informasi sensitif maupun rahasia (Alibeigi, A. and Munir, 2022).

Privasi adalah kondisi atau keadaan bebas dari perhatian publik terhadap gangguan atau campur tangan dengan tindakan atau keputusan seseorang. Privasi sangat berharga karena diyakini melindungi individu dari ancaman eksternal, seperti ejekan, pelecehan, manipulasi, pencurian, subordinasi, pemerasan, dan pengecualian (Katulić, Anita, Tihomir Katulić 2022).

Perlindungan data dan privasi adalah hasil *interplays* yang kompleks dan artikulasi terkait, sulit diidentifikasi, mengenai momen, pilihan lokasi, dan keputusan (Mitrou, 2018).

Sementara itu, dalam praktiknya, privasi adalah konsep lunak berdasarkan persepsi orang tentang risiko dan manfaat. Misalnya, keberadaan kepercayaan publik akan mendapat manfaat saat menggunakan kartu kredit dalam pembelian online yang memberikan kenyamanan lebih besar dibandingkan dengan potensi biaya transaksi data yang disalahgunakan (Acquisti, 2017)

Data pribadi dapat diolah menjadi bentuk data lainnya atau *bentuk big data* atau diolah melalui *cloud computing* (Zanoon, N., Al-Haj, A. and Khwaldeh 2017). *Big data* memerlukan daya komputasi yang tinggi dan penyimpanan yang besar, sistem terdistribusi biasanya digunakan (Hashem et al, 2015). Karena banyak pihak terlibat dalam sistem ini, risiko pelanggaran privasi meningkat. Data pribadi ini dikumpulkan dan ditambang oleh perusahaan seperti *Facebook* , *Google*, perusahaan telepon seluler, jaringan ritel, dan pemerintah (Smith et al, 2012). Ada sejumlah mekanisme pelestarian privasi yang dikembangkan untuk perlindungan privasi pada tahap yang berbeda (misalnya, pembuatan data, penyimpanan data, dan pemrosesan data) dari siklus hidup *big data. Big data* membutuhkan penyimpanan. Teknologi yang digunakan dalam *cloud computing* seperti virtualisasi, penyimpanan dan pemrosesan terdistribusi memiliki memungkinkan untuk melakukan tugas-tugas yang komputasi dan penyimpanan yang besar, yang membawa kebutuhan akan *cloud computing*. *Cloud computing* mendorong perusahaan dan bisnis untuk mengadopsi *cloud*, karena dari banyak keuntungan yang ditawarkannya, seperti penghematan biaya dan skalabilitas. Ini juga menawarkan kekuatan pemrosesan yang besar dan kemampuan telah dipertimbangkan sulit dalam sistem konvensional. Namun, di sisi lain, komputasi awan ini juga dapat menimbulkan masalah privasi. Orang-orang ragu untuk mentransfer pribadi mereka atau data sensitif ke *cloud* kecuali mereka yakin bahwa data mereka akan aman di *cloud* (Mehmood et al, 2016).

Ada beberapa tantangan untuk membangun *big data* yang tepercaya dan aman untuk penyimpanan dan sistem pemrosesan di *cloud* (Mehmood et al. 2016), diantaranya:

- *Outsourcing*: Untuk efisiensi, organisasi saat ini lebih memilih untuk melakukan outsourcing data mereka ke *cloud*. Namun, mengalihdayakan data ke *cloud* juga berarti bahwa pelanggan akan kehilangan fisik kontrol pada data mereka. Hilangnya kendali atas data telah menjadi salah satu penyebab utama ketidakamanan *cloud*. Ketidakamanan dapat menyebabkan kerusakan serius pada privasi pelanggan komputasi awan. Masalah-masalah ini dapat diatasi dengan menyediakan lingkungan komputasi yang aman dan penyimpanan data. Selain itu, data *outsourcing* juga harus dapat diverifikasi kepada pelanggan dalam hal: kerahasiaan dan integritas.
- *Multi-tenancy*: Virtualisasi telah memungkinkan untuk berbagi *platform cloud* yang sama oleh banyak pelanggan. Data milik pengguna *cloud* yang berbeda mungkin ditempatkan pada penyimpanan fisik yang sama oleh beberapa sumber daya kebijakan alokasi. Dalam lingkungan seperti itu, relatif mudah bagi pengguna jahat untuk mengakses data secara ilegal yang bukan miliknya. Serangkaian masalah mungkin terjadi dalam lingkungan seperti itu, seperti pelanggaran data dan pelanggaran perhitungan. Karena itu, sangat penting untuk mekanisme desain untuk menangani potensi privasi dan risiko keamanan.
- Komputasi besar-besaran: Karena kemampuan *cloud* komputasi untuk menangani penyimpanan data besar-besaran dan perhitungan yang intens, mekanisme tradisional untuk melindungi privasi individu tidak cukup (Mehmood et al., 2016). Salah satu solusi yang dapat ditempuh yaitu dengan cara memasang "dinding" keamanan antara *Cloud Server* dan *Internet*, dengan tujuan untuk menghilangkan masalah privasi dan keamanan (Stergiou, Christos, Kostas E. Psannis, Brij B. Gupta 2018).

https://doi.org/10.53276/eligible.v2i1.66

Hubungan Hukum Peminjam *Online* dengan Lembaga Pinjaman *Online*

Hubungan hukum antara Peminjam *Online* dengan Lembaga Pinjaman *Online* tentunya disahkan melalui suatu perjanjian yang diawali dengan persetujuan. Persetujuan yang datur dalam Pasal 1313 KUH Perdata merupakan tindakan atau perbuatan hukum di mana salah satu pihak menawarkan atau memberikan usul, dan pihak lainnya menerima atau menyetujui usul yang ditawarkan tersebut. Jadi dalam persetujuan atau perjanjian yang melahirkan akibat hukum bagi para pihak (Butarbutar and Robert 2021). Peminjam *Online* atau Konsumen atau Pemilik Data Pribadi harus memberikan persetujuan atau pernyataan secara tertulis baik secara manual dan/atau elektronik setelah mendapat penjelasan secara lengkap mengenai tindakan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman,dan penyebarluasan serta kerahasiaan atau ketidakrahasiaan data pribadi (Menteri Komunikasi dan Informatika Republik Indonesia, 2016).

Lebih lanjut, Peminjam *Online* dan lembaga Pinjaman *Online* merupakan subyek hukum yang memiliki hak dan kewajibannya masing-masing. Sesuai dangan Pasal 1320 KUH Perdata, ada 4 (empat) syarat yang harus dipenuhi dalam suatu perjanjian, diantaranya (1) sepakat; (2) kecakapan; (3) adanya suatu hal tertentu; (4) sebab yang halal. Khususnya dalam perjanjian Pinjaman *Online* atau layanan pinjam meminjam uang berbasis teknologi informasi yang merupakan penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi pinjaman dengan penerima pinjaman dalam rangka melakukan perjanjian pinjam meminjam dalam mata uang (Otoritas Jasa Keuangan, 2016). Jika salah satu pihak melakukan pelanggaran maka dapat diselesaikan dengan gugatan wanprestasi jika pelanggaran tersebut menyangkut isi atau obyek perjanjian. Namun jika pelanggarannya menyangkut keadaan atau perbuatan di luar obyek perjanjian maka pihak tersebut dapat dituntut dengan gugatan telah melakukan suatu perbuatan melawan hukum (Butarbutar and Robert, 2021). Oleh karena itu, Peminjam *Online* berhak meminta informasi tentang kejelasan identitas, dasar kepentinan hukum, tujuan permintaan dan penggunaan data pribadi dan akuntabilitas pihak yang meminta data pribadi.

Syarat Pinjaman *Online* umumnya harus memenuhi beberapa syarat, yakni berumur 18 tahun ke atas, melampirkan Kartu Tanda Penduduk (KTP), foto diri sambil memegang KTP untuk keperluan verifikasi, dan syarat lainnya yang ditetapkan sendiri oleh lembaga Pinjaman *Online* (DetikNews, 2020). KTP merupakan data pribadi yang harus dilindungi dalam suatu transaksi. Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Data pribadi dibagi 2 (dua) jenis, *yang pertama*, data pribadi yang bersifat umum yang terdiri dari nama lengkap; jenis kelamin; kewarganegaraan, agama; dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Data pribadi jenis *yang kedua*, yaitu data pribadi yang bersifat spesfik, meliputi: data dan informasi kesehatan; data biometrik; data genetika; kehidupan/oritentasi seksual; pandangan polltik; catatan kejahatan; data anak; data keuangan pribadi; dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan (Indonesia, 2022a).

Dasar Hukum Perlindungan Data Pribadi Konsumen Pinjaman *Online* di Indonesia

Saat ini Perlindungan data pribadi secara spesifik sudah diatur dalam undang-undang. Sebelumnya, perlindungan data pribadi sebagian kecil sudah diatur dalam UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang tercantum dalam Pasal 26 ayat (1) dan (2) yang menyatakan bahwa:

(1) Kecuali ditentukan lain oleh peraturan perundangundangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Ketentuan yang diatur tersebut (Indonesia, 2016), telah memberikan hak kepada pemilik data pribadi untuk tetap menjaga kerahasiaan data pribadinya, apabila data pribadinya telah tersebar dan disalahgunakan oleh pihak lain, maka pemilik data pribadi dapat mengajukan gugatan ke pengadilan. Gugatan yang dimaksud berupa gugatan perdata yang diajukan berdasarkan peraturan perundang-undangan. Ketentuan pasal tersebut merupakan perlindungan yang diberikan terhadap data pribadi seseorang secara umum, artinya dalam setiap kegiatan yang menyangkut transaksi elektronik yang menggunakan data pribadi seseorang maka wajib untuk menjaga dan melindungi data pribadi tersebut, dengan pengaturan tersebut, maka setiap orang memiliki hak untuk menyimpan, merawat dan menjaga kerahasiaan datanya agar data yang dimiliki tetap bersifat pribadi. Setiap data pribadi yang telah diberikan tersebut harus digunakan sesuai dengan persetujuan dari orang yang memiliki dan harus dijaga kerahasiaannya (Nurmantari and Martana, 2020).

Lebih lanjut, dalam Pasal 26 huruf a POJK No.77/POJK.01/2016 mewajibkan penyelenggara untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan. Hal ini berarti pihak pemberi pinjaman memiliki kewajiban untuk merahasiakan data pribadi peminjam dimulai dari proses perjanjian pinjam-meminjam dibuat hingga selesainya perjanjian tersebut. Kewajiban tersebut harus dilaksakan guna tercapainya perlindungan terhadap data pribadi peminjam. Demikian juga Pasal 26 huruf c POJK ini menyatakan bahwa penyelenggara wajib menjamin bahwa perolehan, penggunaan, pemanfaatan, dan pengungkapan data pribadi yang diperoleh oleh Penyelenggara berdasarkan persetujuan pemilik data pribadi, data transaksi, dan data keuangan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan. Berdasarkan pasal tersebut jelas bahwa, tanpa persetujuan dari pemilik data pribadi. Kemudian Pasal 28 ayat (3) POJK 77/2016 dalam mendukung keamanan teknologi informasi dalam industri jasa keuangan, Penyedia (Lembaga Jasa Keuangan Lainnya) harus berpartisipasi dalam mengelola celah keamanan. Untuk alasan ini, Penyedia harus menampilkan dokumen elektronik lengkap mengikuti format dan periode penyimpanan yang ditentukan mengikuti ketentuan perundang-undangan (Butarbutar 2020).

Namun paradoksnya, dalam Pasal 23 POJK 77/201 diatur bahwa Penyedia dapat berkolaborasi dan bertukar data dengan penyedia layanan dukungan berbasis teknologi informasi untuk meningkatkan kualitas layanan Pinjaman P2P yang cenderung mengakibatkan penyalahgunaan pertukaran data pribadi. Untuk alasan ini, penting untuk mengetahui bagaimana hukum dan peraturan di Indonesia melindungi penyalahgunaan pertukaran data pribadi, terutama dalam platform pinjaman *online*. Pihak utama dalam skema pinjaman P2P adalah penyedia, peminjam, dan pemberi pinjaman, yang dimanifestasikan dalam dua jenis perjanjian, yaitu perjanjian antara penyedia dan pemberi pinjaman, dan perjanjian antara pemberi pinjaman dan peminjam yang dilakukan secara elektronik (ABNR Counsellors At Law 2017).

Lebih lanjut, Undang-Undang Perlindungan Konsumen mengatur segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen. Konsumen disini merupakan Peminjam *Online* atau Pemilik Data Pribadi sebagai pemakai barang dan/atau jasa. Pasal 7 mewajibkan pelaku usaha atau Lembaga Pinjaman *Online* untuk selalu beritikad baik dalam melakukan kegiatan usahanya, memberikan informasi yang benar,

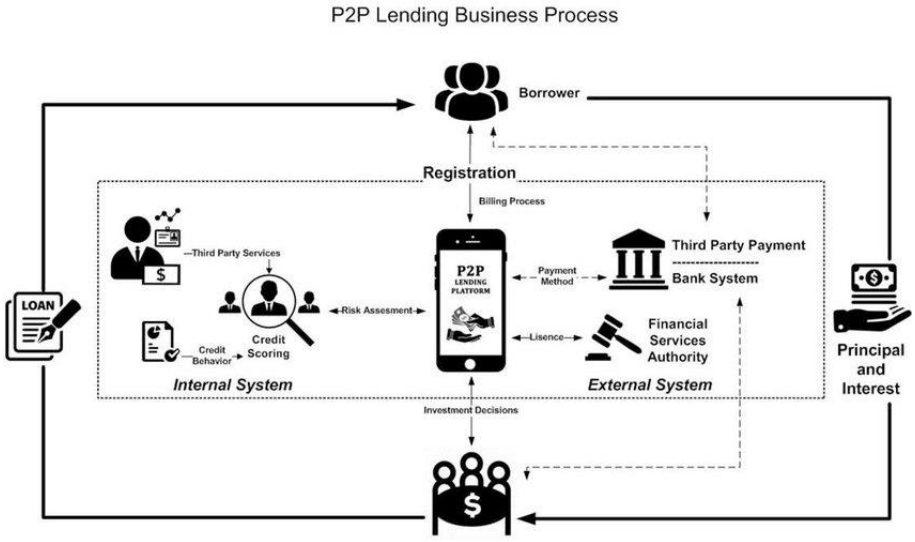
https://doi.org/10.53276/eligible.v2i1.66

jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan. Kemudian memberi kompensasi, ganti rugi, dan atau penggantian apabila barang dan/atau jasa yang diterima untuk dimanfaatkan tidak sesuai dengan perjanjian (Indonesia, 1999).

Dari pengaturan hukum yang dijelaskan di atas, belum ada aturan hukum yang spesifik yang mengatur tentang perlindungan data pribadi untuk pinjaman online. Oleh karena itu dibutuhkan suatu undang-undang yang khusus untuk perlindungan data pribadi. Dalam perkembangannya atau berita baiknya, Indonesia saat ini dalam perkembangannya, telah memiliki melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini berfungsi untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat atas pentingnya perlindungan data pribadi (Indonesia, 2022b).

Bagaimana Seharusnya Perlindungan Data Pribadi Konsumen Pinjaman *Online*?

Perlindungan data pribadi khususnya konsumen pinjaman *online* menjadi sangat penting untuk segera diatur dan diundangkan karena proses bisnisnya yang menyangkut banyak pihak. Data pribadi yang dikelola melalui sistem internal dan eksternal dan kemungkinan adanya pihak ketiga yang ikut dalam proses bisnis dimaksud sehingga pemrosesan dan peredaran data pribadi bisa sampai ke pihak yang tidak bertanggung jawab (Lihat Gambar 1). Secara pribadi penting untuk melakukan prinsip kehati-hatian terkait data pribadi khususnya terkait pemrosesan data pribadi yang meliputi: (1) pembatasan cara pengumpulan, penyimpanan atau pembagian data pribadi; (2) mewajibkan perusahaan untuk mengungkapkan cara mereka menggunakan data pribadi; (3) mengamanatkan tingkat mimimun perlindungan data pribadi. Uni Eropa menurut Peraturan Perlindungan Data Umum atau *General Data Protection Regulation* (GDPR) mengharuskan perusahaan memberikan informasi yang transparan tentang data pribadi yang mereka kumpulkan dari konsumen; mengizinkan pengumpulan, penyimpanan, atau pembagian data pribadi hanya berdasarkan dasar hukum tertentu; dan menerapkan perlindungan tingkat tinggi atas data pribadi. GDPR mengharuskan bisnis (dan organisasi lain) menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan tingkat keamanan atas data pribadi (TermsFeed 2021).



Gambar 1 Proses Bisnis Pinjaman Online (Suryono, Purwandari, and Budi 2019)

Jika terjadi kegagalan dalam melakukan perlindungan data pribadi, maka dapat mengakibatkan peringatan, denda, dan hukuman lainnya dari Otoritas Perlindungan Data. Besaran denda tersebut bisa berupa apa saja hingga €20 juta atau empat persen dari omset tahunan perusahaan Anda (mana yang lebih besar). GDPR berlaku di setiap negara UE (termasuk Inggris Raya), yang telah menerapkannya melalui undang-undang nasional mereka sendiri. Misalnya, pada tahun 2015, pengecer Inggris *Carphone Warehouse* mengalami pelanggaran data di mana data pribadi tiga juta pelanggan dikompromikan. Perusahaan didenda £400.000 di bawah undang-undang pra-GDPR Inggris karena gagal, untuk menguji dan memelihara sistem keamanan datanya (TermsFeed, 2021).

Sesuai dengan aturan GDPR, setiap pemrosesan data pribadi harus sah dan adil. Harus transparan kepada orang-orang alami bahwa data pribadi mereka dikumpulkan, digunakan, dikonsultasikan, atau diproses dengan cara lain dan sejauh mana: data pribadi sedang atau akan diproses. Prinsip transparansi mensyaratkan bahwa setiap informasi dan komunikasi yang berkaitan dengan pemrosesan data pribadi tersebut dapat diakses dengan mudah dan mudah dipahami, serta jelas dan bahasa yang biasa digunakan. Prinsip itu menyangkut, khususnya, informasi kepada subjek data tentang identitas pengontrol dan tujuan pemrosesan dan informasi lebih lanjut untuk memastikan keadilan dan pemrosesan yang transparan sehubungan dengan orang perseorangan yang bersangkutan dan hak mereka untuk memperoleh konfirmasi dan komunikasi data pribadi mengenai mereka yang sedang diproses. Orang alami harus dibuat sadar akan risiko, aturan, perlindungan, dan hak terkait dengan pemrosesan data pribadi dan cara menggunakannya hak sehubungan dengan pemrosesan tersebut. Secara khusus, tujuan khusus pemrosesan data pribadi harus eksplisit dan sah dan ditentukan pada saat pengumpulan data pribadi. Data Pribadi harus memadai, relevan, dan terbatas pada apa yang diperlukan untuk tujuan pemrosesannya. Hal ini memerlukan, khususnya, memastikan bahwa periode penyimpanan data pribadi dibatasi pada batasan yang ketat minimum. Data pribadi harus diproses hanya jika tujuan pemrosesan tidak dapat secara wajar dipenuhi dengan cara lain. Untuk memastikan bahwa data pribadi tidak disimpan lebih lama dari yang diperlukan, batas waktu harus ditetapkan oleh pengontrol untuk penghapusan atau untuk tinjauan berkala. Setiap langkah yang logis harus diambil untuk memastikan bahwa data pribadi yang tidak akurat diperbaiki atau dihapus. Data pribadi harus diproses dalam cara yang menjamin keamanan dan kerahasiaan data pribadi yang sesuai, termasuk untuk mencegah akses tidak sah ke atau penggunaan data pribadi dan peralatan yang digunakan untuk pemrosesan (European Parliament, 2016).

Untuk merealisasikan perlindungan data pribadi tentunya membutuhkan Pengendali Data Pribadi yang berfungsi untuk melakukan kendali pemrosesan data pribadi, dan Prosesor Data Pribadi atau pihak yang melakukan pemrosesan data pribadi atas nama Pengendali Data Pribadi. Sehingga kepastian hukum tentang pemrosesan data pribadi dapat dilakukan secara akurat dan transparan. Dengan demikian hak-hak pemilik data pribadi dapat lebih terjamin terkait dengan hak untuk: (1) mengakhiri pemrosesan, menghapus dan/atau memusnahkan data ptibadi miliknya; (2) menarik kembali persetujuan pemrosesan data pribadi miliknya yang telah diberikan kepada Pengendali Data Pribadi; (3) mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*); (4) memilih atau tidak memilih pemrosesan data pribadi melalui mekanisme *pseudonim* untuk tujuan tertentu; (5) menunda atau membatasi pemrosesan data pribadi secara proporsional sesuai dengan tujuan pemrosesan data pribadi; (6) menuntut dan menerima ganti rugi atas pelanggaran data pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan; (7) mendapatkan dan/atau menggunakan data pribadi miliknya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik atau perangkat keras yang digunakan dalam

https://doi.org/10.53276/eligible.v2i1.66

interoperabilitas antar sistem elektronik; (8) menggunakan dan mengirimkan data pribadi miliknya ke Pengendali Data Pribadi lainnya, sepanjang sistem tersebut dapat saling berkomunikasi secara aman sesuai dengan prinsip perlindungan data pribadi (Indonesia 2022a).

Larangan dan Sanksi Hukum Terhadap Pelanggaran Perlindungan Data Pribadi

Larangan dalam penggunaan data pribadi ditujukan kepada orang yang memperoleh atau mengumpulan atau mengungkapkan atau menggunakan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian pemilik data pribadi atau konsumen. Demikian juga dengan larangan jual beli data pribadi, memalsukan data pribadi, menggunakan alat pengolah data visual secara melawan hukum untuk mengidentifikasi seseorang (Indonesia, 2022a).

Sanksi hukum terkait pelanggaran perlindungan data pribadi biasanya meliputi sanksi administratif dan sanksi pidana. Untuk sanksi administratif umumnya dikenakan: (1) peringatan tertulis; (2) Pengehentian sementara kegiatan pemrosesan data pribadi: (3) penghapusan dan pemusnahan data pribadi; (4) ganti kerugian; dan/atau; (5) denda administratif. Sementara untuk sanksi pidana harus disesuaikan dengan berat ringannya pelanggaran atau tindak pidana yang dilakukan yang bisa direalisasikan dengan sanksi pidana penjara dan/atau pidana denda yang sepadan (Indonesia, 2022a).

KESIMPULAN

Perlindungan hukum tentang data pribadi khususnya Konsumen Pinjaman *Online* di Indonesia perlu untuk segera direalisasikan melalui pengesahan Peraturan Pemerintah dan/atau Undang-Undang tentang Perlindungan Data Pribadi untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Aturan hukum dimaksud harus bisa menjamin perlindungan data secara akurat dan transparan serta mengatur tentang (1) pembatasan cara pengumpulan, penyimpanan atau pembagian data pribadi; (2) kewajiban perusahaan untuk mengungkapkan cara mereka menggunakan data pribadi; (3) mengamanatkan tingkat mimimun perlindungan data pribadi; (4) jaminan hukum terhadap hak pemilik data pribadi; (5) larangan dalam penggunaan data pribadi ditujukan kepada orang yang memperoleh atau mengumpulan atau mengungkapkan atau menggunakan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian pemilik data pribadi atau konsumen; (6) perumusan sanksi administratif dan sanksi pidana yang berkeadilan, berkepastian, dan bermanfaat secara hukum. dan ekonomi.

UCAPAN TERIMA KASIH

Terima kasih kami ucapkan kepada Fakultas Hukum Universitas Bung Karno, dan Kantor Advokat Russel Butarbutar and Partners.

REFERENSI

ABNR Counsellors At Law. 2017. “OJK’s Regulation on Financial Technology-Based Lending Services.” 2017. https://www.lexology.com/library/detail.aspx?g=0b387cf6-5564-4f5c-

a9cd-8c202e26936e.

Acquisti, A . et al. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." *ACM Computing Surveys (CSUR)* 50 (3): 1–41.

Alibeigi, A. and Munir, A.B. 2022. "A Decade after the Personal Data Protection Act 2010 (PDPA): Compliance of Communications Companies with the Notice and Choice Principle." *Journal of Data Protection & Privacy* 5 (2): 119–37.

Benuf, Kornelius, and Muhamad Azhar. 2020. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7 (1): 20–33.

Bisnis Indonesia. 2021. "RUU Perlindungan Data Pribadi : China Sudah Teken, RI Kapan?" 2021. https://bisnisindonesia.id/article/ruu-perlindungan-data-pribadi-china-sudah-teken-ri-kapan.

Butarbutar, Russel. 2020. "Personal Data Protection in P2P Lending: What Indonesia Should Learn from Malaysia?" *Pertanika* 28 (3): 2295–2307.

Butarbutar, Russel, and Robert. 2021. *Hukum Perdata Di Indonesia: Kompilasi, Penerapan, Dan Tantangan Hukum Kedepannya*. Bekasi: Gramata Publishing.

Dataguidance.com. 2022. "EU - Data Protection Overview." 2022. https://www.dataguidance.com/notes/eu-data-protection-overview.

DetikNews. 2020. "Syarat Ajukan Pinjaman Online, Dari Pinjol Legal Hingga KUR BRI." 2020. https://www.detik.com/jateng/bisnis/d-6204043/syarat-ajukan-pinjaman-online-dari-pinjol-legal-hingga-kur-bri#:~:text=Syarat Ajukan Pinjaman Online di Pinjol Legal&text=Sudah berusia legal (18 tahun,dari karyawan hingga pelaku bisnis.

Dewayani, Tantri. 2021. "Menyikapi Pinjaman Online, Anugerah Atau Musibah." 2021. https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/14040/Menyikapi-Pinjaman-Online-Anugerah-atau-Musibah.html.

European Parliament. 2016. *Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (GDPR)*.

Hasela, Rizka Noor. 2020. "Lemahnya Perlindungan Hukum Bagi Nasabah Pinjaman Online." 2020. https://jdih.tanahlautkab.go.id/artikel_hukum/detail/lemahnya-perlindungan-hukum-bagi-nasabah-pinjaman-online.

Hashem, Ibrahim Abaker Targio, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. 2015. "The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues." *Information Systems* 47: 98–115.

Hutsix. 2021. "Data Protection Act's Eight Principles (And Why Are There Now Only Seven?)." 2021. https://www.hutsix.io/what-are-the-eight-principles-of-the-data-protection-act/.

Indonesia. 1999. *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*.

———. 2016. *Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*.

———. 2022a. *Rancangan Undang-Undang Republik Indonesia Tentang Perlindungan Data Pribadi*.

———. 2022b. *Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*.

Kantaatmadja (et al), Mieke Komar. 2002. *Cyberlaw: Suatu Pengantar*. Bandung: Eclips II.

Katulić, Anita, Tihomir Katulić, and Ivana Hebrang Grgić. 2022. "Application of the Principle of Transparency in Processing of European National Libraries Patrons' Personal Data." *Digital Library Perspectives*.

Makarim, Edmon. 2003. *Kompilasi Hukum Telematika*. Jakarta: PT RajaGrafindo Persada.

https://doi.org/10.53276/eligible.v2i1.66

Mehmood, A, I Natgunanathan, Guang HUa, and Song Guo. 2016. "Protection of Big Data Privacy." *IEEE Access* 4: 1821–34.

Menteri Komunikasi dan Informatika Republik Indonesia. 2016. *Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik*.

Mitrou, Lilian. 2018. "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof'?" *Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof*.

Nurmantari, Ni Nyoman Ari Diah, and Nyoman A. Martana. 2020. "Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online." *Fakultas Hukum Universitas Udayana*, 1–14.

Okezone. 2021. "Berikut Daftar Negara Punya UU Perlindungan Data Pribadi, Denda Rp356 Miliar Menanti!" 2021. https://nasional.okezone.com/read/2021/05/31/337/2418183/berikut-daftar-negara-punya-uu-perlindungan-data-pribadi-denda-rp356-miliar-menanti.

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

Pratiwi, Tiara Hana. 2021. "Pentingnya Pelindungan Data Pribadi Di Era Digital." 2021. https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/.

Priscyllia, Fanny. 2019. "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum." *Jatiswara* 34 (3): 239–49.

QuestionPro. 2020. "Qualitative Research: Definition, Types, Methods and Examples." 2020. https://www.questionpro.com/blog/qualitative-research-methods/.

Smith, M., C. Szongott, B. Henne, and G. Von Voigt. 2012. "Big Data Privacy Issues in Public Social Media." In *6th IEEE International Conference on Digital Ecosystems and Technologies (DEST) (Pp. 1-6)*.

Stergiou, Christos, Kostas E. Psannis, Brij B. Gupta, and Yutaka Ishibashi. 2018. "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT." *Sustainable Computing: Informatics and Systems* 19 (174–184).

Suryono, Ryan Randy, Betty Purwandari, and Indra Budi. 2019. "Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review." In *The Fifth Information Systems International Conference 2019*, 204–214.

TermsFeed. 2021. "Protecting Personal Data in Your Business." 2021. https://www.termsfeed.com/blog/protect-personal-data-business/.

Wrigley, Sam. 2019. *"'When People Just Click': Addressing the Difficulties of Controller/Processor Agreements Online." In Legal Tech, Smart Contracts and Blockchain*. Singapore: Springer.

Yuwono, Felix, Emanuel Raja Damaitu, and Sheila Yudha Pradina. 2021. "Online Dispute Resolution Dalam Sengketa Bisnis Di Era Digital: Sebuah Konsep Dengan Pendekatan Perbandingan Hukum." *Journal of Private and Economic Law* 1 (2): 199–231.

Zanoon, N., Al-Haj, A. and Khwaldeh, S.M. 2017. "Cloud Computing and Big Data Is There a Relation between the Two: A Study." *International Journal of Applied Engineering Research* 12 (17): 6970–82.