Jurnal Yustika dapat diunduh pada website berikut:
http://journal.ubaya.ac.id/index.php/yustika

Tinjauan Yuridis Perbuatan Melanggar Hukum (PMH) Penyalahgunaan Data Pribadi Aplikasi di Google Play Store

Anisa Isti Briliany (a), Anajeng Esri Edhi Mahanani (b)

(a) Universitas Pembangunan Nasional Veteran Jawa Timur, nisabriliany@gmail.com
(b) Universitas Pembangunan Nasional Veteran Jawa Timur, anajengmahanani.ih@upnjatim.ac.id

Abstract

The industrial revolution 4.0 in Indonesia can be seen by the massive use of the internet in people's daily activities through electronic systems in the form of applications for searching information, socializing and commercial activities. Access of applications become easier by installing on smartphones that are supported by one of the best known operating systems, which is Android with Google Play Store as digital application service provider. However, behind all the conveniences some applications demand a lot of user personal data such as detailed user financial information to continue transactions. It has the risk of violating the law that injures the rights of others due to violating laws and regulations, or violating the interests of others as specified in Article 1365 of the Civil Code. Through this research, it can be identified that there are forms of unlawful acts that occur for the misuse of personal data, namely vulnerabilities in data security, lack of transparency over the fate of data through notifications, and administrative defects in providing applications. The three types of unlawful acts are reviewed based on the applicable regulations including Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019 concerning System Operations and Electronic Transactions, and Google Play Store regulations. The existence of these legal facts certainly threatens the security of users, therefore the law as a protector presents a dispute resolution solution for this matter, either through litigation or non-litigation.

Keywords: unlawful act; transparency; personal data.

Abstrak

Kehadiran revolusi industri 4.0 di Indonesia dapat terlihat dengan masifnya penggunaan internet dalam kegiatan sehari-hari masyarakat seperti mencari informasi, bersosialisasi maupun melakukan kegiatan jual-beli melalui sistem elektronik berupa situs web serta aplikasi. Akses dalam memperoleh aplikasi jugalah sangat mudah dengan mengunduh aplikasi pada gawai pribadi layaknya *smart phone* yang didukung dengan salah satu sistem operasi, salah satunya yang paling dikenal di dunia ialah Android dengan Google Play Store sebagai penyedia layanan aplikasi digital guna mendistribusikan berbagai macam aplikasi. Namun dibalik segala kemudahan yang ditawarkan, dalam beberapa aplikasi banyak data pribadi pengguna seperti identitas lengkap hingga informasi keuangan pengguna dibutuhkan agar dapat melanjutkan kegiatan elektronik. Tindakan tersebut dapat menimbulkan perbuatan melanggar hukum dikarenakan melanggar peraturan perundang-undangan ataupun melanggar kepentingan orang lain sebagaimana Pasal 1365 KUHPerdata. Penelitian ini dilangsungkan menggunakan penelitian hukum yuridis-normatif dengan mengkaji data berupa peraturan perundang-undangan yang berlaku, mencangkup Undang-Undang Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan regulasi Google Play Store dalam bentuk kebijakan pengembang

Jurnal
YUSTIKA
Media Hukum dan Keadilan
Fakultas Hukum Universitas Surabaya
Vol. 24 No. 02, Desember 2021
P-ISSN: 1410-7724
E-ISSN: 2655-7479

program serta perjanjian distribusi pengembang. Berdasarkan penelitian ini dapat diidentifikasikan terdapat bentuk-bentuk perbuatan melanggar hukum yang terjadi atas penyalahgunaan data pribadi para pengguna mencangkup kerentanan kemanan data pribadi, minimnya transparansi atas nasib data pribadi melalui penulisan notifikasi, serta cacat administrasi penyediaan aplikasi. Adanya fakta hukum tersebut tentunya mengancam keamanan para pengguna, oleh karenanya hukum sebagai pelindung menghadirkan solusi penyelesaian sengketa atas hal tersebut baik melalui jalur litigasi ataukah non-litigasi.
Kata Kunci: Perbuatan melanggar hukum; transparansi; data pribadi.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi semakin canggih didorong dengan kondisi global yang menghendaki pemanfaatan internet secara besar-besaran, peristiwa tersebut menjadikan masyarakat dunia khususnya masyarakat Indonesia menjadi pengguna internet aktif dimana pada tahun 2021 sebanyak 202.6 juta jiwa masyarakat Indonesia dari 274,9 juta jiwa merupakan pengguna aktif internet, dari jumlah tersebut 195.3 juta jiwa penduduk Indonesia mengakses internet dengan perangkat *mobile* (Kemp, 2021). Data tersebut menunjukkan bahwa banyak masyarakat lebih nyaman mengakses internet menggunakan *smartphone* dikarenakan lebih praktis dan mudah untuk digunakan oleh banyak kalangan.

Salah satu sistem operasi paling dikenal di Indonesia dan dunia yakni Android, hadir didalam berbagai macam merek *smartphone* maupun tablet yang dibangun dengan fitur menarik dan mudah untuk digunakan oleh berbagai kalangan., dimana dalam menggunakan perangkat berbasis sistem Android maka pengguna akan disuguhkan berbagai aplikasi yang dengan sendirinya terdapat pada ponsel, selain itu pengguna *smartphone* berbasis Android dapat mengunduh berbagai macam aplikasi lain yang menarik melalui fitur Google Play Store. Google Play Store sendiri menyajikan berbagai macam konten aplikasi yang dibuat oleh beragam pihak yang mengembangkan konten aplikasi seperti aplikasi mengedit foto dan permainan yang bersifat hiburan, pinjaman online atau *fintech* sebagai bagian digitalisasi keuangan, serta berbagai macam aplikasi *e-commerce* atau toko online yang memudahkan masyarakat bertransaksi jual-beli secara instan tanpa perlu bertatap muka. Kegiatan yang semula memerlukan keterlibatan ataukah bantuan orang lain dalam bentuk fisik beralih tergantikan dengan bantuan aplikasi sebagai bentuk sistem elektronik, hal tersebut menjadi suatu dinamika kehidupan berupa kemudahan dalam melakukan berbagai hal yang akhirnya menjadi gaya hidup masyarakat.

Kepraktisan dari penggunaan aplikasi tersebut menyimpan risiko yang cukup besar didalamnya terutama faktor keamanan data yang dihimpun oleh aplikasi tertentu dengan mensyaratkan pencantuman berbagai data pribadi seperti nama, alamat e-mail, nomor telepon, alamat, ataupun data nomor rekening bank jika melakukan transaksi pembayaran pada aplikasi *e-commerce*. Sesungguhnya data pribadi tersebut meski terkesan umum untuk diketahui memuat informasi yang memiliki nilai pribadi bagi pemiliknya yang oleh Samuel Garfunkel disebut sebagai informasi pribadi yang diklasifikasikan kedalam 5 (lima) jenis berupa informasi personal yang bersifat generik layaknya nama dan umur, informasi privat yang tidak diketahui secara umum semisal catatan perbankan dan transkrip akademik, informasi identifikasi pribadi berupa informasi yang telah disimpulkan oleh seseorang berupa kebiasaan ataupun hal yang digemari, informasi anonim yang merupakan informasi yang telah ditransformasi sedemikian rupa

sehingga informasi yang diperoleh bukan informasi yang sebenarnya, serta informasi agregat yang merupakan kumpulan dari informasi beberapa individu (Dewi, 2009).

Pencantuman beberapa data pribadi tersebut memiliki berbagai risiko tinggi terkait pelanggaran data *(data breach)* seperti kebocoran data kepada dunia luas baik sengaja maupun tidak sengaja ataukah pemanfaatan data yang tidak sesuai dengan tujuan awal dihimpunnya data tersebut. Permasalahan terkait keamanan data pribadi di Indonesia dan dunia cukup banyak terjadi, salah satunya di Indonesia pada aplikasi Cermati yang merupakan aplikasi teknologi finansial mengalami kebocoran data yang dilakukan oleh pihak eksternal untuk dijual (Clinten, 2020). Penyalahguanaan data tidak hanya dapat terjadi pada aplikasi milik perusahaan *start up* saja tetapi juga dapat terjadi pada aplikasi milik perusahaan dunia, Facebook sebagai pelopor media sosial pada awal tahun 2018 mengakui bahwa terjadi pemanfaatan informasi data privasi pengguna dengan memberikan informasi pengguna pada konsultan politik Cambridge Analytica untuk dapat menargetkan iklan kampanye yang disesuaikan berdasarkan profil psikologis pengguna Facebook (Criddle, 2020). Selain itu pada awal kondisi pandemi Covid-19 terdapat kejadian yang berlangsung terkait keamanan data pribadi dialami oleh aplikasi Zoom dimana pada bulan April 2020 aplikasi tersebut dinilai memiliki celah besar terjadinya pelanggaran data pribadi penggunanya, dimana pakar keamanan siber data Pratama Persadha menghkawatirkan terjadinya praktik penyalahgunaan data pemetaan wajah data (Karo-Karo and Prasetyo, 2020), pemetaan wajah tersebut dikhawatirkan dapat disalahgunakan untuk membuka sandi perangkat elektronik yang menggunakan fitur *Face Id*.

Pemerolehan rasa aman dalam pemakaian suatu aplikasi haruslah didapatkan oleh pengguna saat menggunakan aplikasi tersebut, hal tersebut dapat diwujudkan dengan pembuatan sistem aplikasi yang aman diikuti dengan proses manajemen risiko yang baik serta transparan. Kejelasan atas data pribadi dalam aplikasi tersebut dapat disajikan dengan cara mencantumkan bagaimana data yang diperoleh akan digunakan yang dituliskan dalam bentuk kebijakan privasi ataukah *privacy policy*. Hadirnya kebijakan privasi tersebut sebagai bentuk pengakuan pengembang aplikasi dengan dilindunginya data pengguna saat mencantumkan informasi pribadinya sebagaimana amanat dalam Pasal 3 Ayat (1) Peraturan Pemerintah No 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronikyakni, setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Kenyataan yang terjadi tidak semua pengembang aplikasi memerhatikan hal tersebut, dimana masih ditemukan pengembang aplikasi yang tidak menyelenggarakan aplikasi yang memenuhi standar keamanan pengguna, maupun tidak mencantumkan *privacy policy* sehingga pengguna tidak mendapatkan jaminan atas keamanan informasi data pribadinya yang seharusnya ia peroleh sebagai hak yang patut didapatkan.

Berdasarkan uraian diatas maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana kriteria perbuatan melanggar hukum (PMH) terkait penyalahgunaan data pribadi?
2. Bagaimana upaya penyelesaian sengketa bagi pengguna aplikasi pada Google Play Store yang mengalami penyalahgunaan data pribadi?

2. MetodePenelitian

Penelitian dilakukan menggunakan jenis penelitian Yuridis Normatif yang merupakan penelitian hukum dengan mengkaji bahan pustaka ataukah data sekunder sebagai acuan

utama (Waluyo, 2008). Penerapan jenis penelitian Yuridis Normatif dimaksudkan untuk pemerolehan gambaran yang jelas mengenai aspek perbuatan melanggar hukum atas data pribadi pengguna aplikasi.

3. Hasil Penelitian dan Pembahasan

3.1 Kriteria Perbuatan Melanggar Hukum (PMH) Terkait Penyalahgunaan Data Pribadi

Perbuatan Melanggar Hukum sebagai terminologi telah dikenal dalam dunia hukum sejak lama terbukti dengan ditemukannya peraturan terkait perbuatan melanggar hukum pada Kitab Hukum Hammurabi yang dibuat pada tahun 1750 SM. Cangkupan perbuatan yang termasuk dalam kategori perbuatan melanggar hukum pada dahulu kala sebelum memasuki tahun 1919 hanyalah terbatas dengan aturan perundang-undangan yang berlaku saja, sesuai dengan Pasal 1365 KUHPerdata ataukah Pasal 1401 BW Belanda dimana perbuatan yang tidak diatur dalam undang-undang dianggap tidak memenuhi klasifikasi perbuatan melanggar hukum sehingga tidak dapat dijatuhi hukuman atas perbuatan tersebut. Namun hal itu telah tergantikan semenjak tahun 1919 sejak terjadinya yurisprudensi atas putusan Mahkamah Agung Belanda (Hoge Raad) atas kasus Lidenbaum melawan Cohen (Arrest Lidenbaum-Cohen) dimana klasifikasi perbuatan melanggar hukum mengalami perluasan makna, tidak hanya terhadap hal yang telah diatur dalam undang-undang saja melainkan juga terhadap perbuatan yang bersinggungan dengan hak orang lain, perbuatan yang bertentangan dengan kewajiban hukum pelaku, maupun perbuatan yang bertentangan prinsip pergaulan yang baik pada masyarakat, dan juga bertentangan dengan kesusilaan (Fuady, 2017, 6).

Sebuah perbuatan untuk dapat diklasifikasian sebagai perbuatan melanggar hukum haruslah menciderai hak orang lain, dimana perbuatan tersebut tentunya melanggar peraturan perundang-undangan yang berlaku, menyebabkan kerugian, melanggar kewajiban hukum pelaku, melanggar kesusilaan *(geode zeden)*, ataukah bertentangan dengan kepentingan orang lain (Fuady, 2017, 11). Ke-lima poin tersebut merupakan kriteria utama untuk dapat melihat perbuatan tersebut sebagai perbuatan melanggar hukum. Selain itu untuk menilai apakah suatu perbuatan dapat dikondisikan kedalam perbuatan melanggar hukum maka perlu memenuhi unsur didalamnya, berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata perbuatan melanggar hukum wajib memenuhi unsur sebagai berikut:

1. Adanya suatu perbuatan
   Perbuatan yang dimaksudkan meliputi perbuatan dalam arti aktif yakni berbuat sesuatu maupun dalam arti pasif yakni tidak berbuat sesuatu seperti tidak mengindahkan kewajiban yang timbul dari ketentuan hukum yang ada. Perbuatan dapat dicontohkan dimana dalam membuat aplikasi berkaitan kegiatan ekonomi agar dapat dipakai oleh khalayak umum maka diperlukan proses pendaftaran didalamnya, proses pendaftaran tersebut ialah perbuatan.
2. Perbuatan merupakan perbuatan melanggar hukum
   Istilah perbuatan melanggar hukum sejak adanya putusan pada tahun 1919 mengalami perluasan makna, adapun perbuatan melanggar hukum tersebut meliputi perbuatan yang melanggar undang-undang, perbuatan yang melanggar hak orang lain, perbuatan yang bertentangan dengan kewajiba hukum pelaku, perbuatan yang bertentangan

Jurnal Yustika
Vol. 24 No. 02, Des 2021

dengan kesusilaan dan perbuatan yang bertentangan dengan sikap baik dalam lingkungan masyarakat. Sebagai contoh dalam sebuah aplikasi diwajibkan penulisan pemberitahuan atau notifikasi terkait persetujuan atas akses data pribadi yang diminta, namun nyatanya tidak semua aplikasi memberikan notifikasi yang transparan sehingga perbuatan tersebut merupakan perbuatan melanggar hukum.

3. Terdapat kesalahan
   Unsur kesalahan *(schuldelement)* menjadi syarat wajib untuk dapat diklasifikasikan dalam perbuatan melanggar hukum, dimana kesalahan tersebut harus memenuhi syarat adanya kesengajaan ataukah adanya kelalaian *(culpa)* yang dimana kesengajaan atau kelalaian tersebut tidak terdapat alasan pembenar diantaranya seperti force meijure, membela diri dan sakit jiwa. Sebagai contoh peristiwa kebocoran data privasi tidak dapat dilepaskan dari adanya unsur kesalahan pemilik aplikasi yang lalai untuk tidak menerapkan keamanan dengan lebih baik.
4. Terdapat kerugian
   Kerugian yang timbul atas suatu perbuatan melanggar hukum meliputi kerugian materiil seperti biaya yang dirugikan maupun imateeril, hal ini menjadi pembeda dengan kerugian akibat wanprestasi yang hanya mengenal kerugian materiil saja. Sebagai contoh bocornya data pribadi mengakibatkan para pengguna mengalami kerugian berupa rasa ketakutan serta kemungkinan penyalahgunaan data yang beredar.
5. Terdapat hubungan kausal antar perbuatan dengan kerugian
   Hubungan kausal antar perbuatan dengan kerugian yang dialami memiliki arti bahwa perbuatan seseorang menjadi sebab atas kerugian orang lain dikarenakan kerugian tidak akan terjadi tanpa penyebab, contohnya ialah gangguan yang dialami pengguna gawai berupa terror telemarketing bisa jadi disebebkan karena adanya perbuatan melanggar hukum berkaitan kebocoran data (Munir, 2017).

Kegiatan transaksi elektronik melalui aplikasi telah beberapa kali mengalami kejadian perbuatan melanggar hukum berkaitan dengan rentannya data pribadi dimana perbuatan tersebut tidak hanya melanggar peraturan perundang-undangan saja melainkan juga melanggar ketentuan yang ada dalam Google Play Store, adapun beberapa bentuk tindakan perbuatan melanggar hukum tersebut meliputi:

a. Kerentanan keamanan data pribadi pada aplikasi.

Keamanan atas data pribadi sejatinya merupakan hak dasar bagi para pengguna aplikasi yang harus diwujudkan oleh penyelenggara sistem elektronik, dimana hal tersebut jugalah dijamin dalam payung hukum perundang-undangan di Indonesia tepatnya Pasal 11 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pemerolehan rasa aman bagi pengguna atas data pribadinya diwujudkan oleh pihak pembuat aplikasi dengan cara menerapkan prinsip perlindungan data pribadi sesuai Pasal 14 (1) Peraturan Pemerintah *A Quo*, pengumpulan maupun tujuan pengambilan data dilakukan secara spesifik sesuai tujuan, diikuti dengan tindakan perlindungan keamanan dari kehilangan, penyalahgunaan data pribadi maupun pemberitahuan atas data pribadi tersebut. Alasan mengapa keamanan atas data pribadi wajib dipenuhi oleh para penyelenggara sistem ialah dikarenakan informasi berupa data pribadi dapat memberikan gambaran mendalam atas hubungan pemilik data tersebut dengan seseorang, sehingga menjadi alat pemetaan *(instrumental mapping)* yang sangat berharga dikarenakan menggambarkan pribadi dan ketertarikan individual yang bernilai komersil (Priowirjanto, 2019), selain itu data pribadi milik masyarakat

Indonesia yang berkaitan dengan kependudukan layaknya Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk Elektronik (E-KTP), maupun Kartu Keluarga (KK) memiliki arti yang sangat penting dikarenakan memiliki peran penting dalam mengidentifikasi seseorang sebagai warga negara, sehingga wajib dilindungi dari segala bentuk penyalahgunaan data seperti *profiling*, tindakan spionase ataukah tujuan perdagangan (Sautunnida, 2018).

Sebagaimana yang dilaporkan oleh Motherboard Vice (Cox, 2020) aplikasi Muslimpro sempat diketahui menjual data lokasi, nama jaringan serta model ponsel para penggunanya kepada perusahaan X-Mode, yakni perusahaan yang menjual informasi kepada konsumennya yang merupakan pihak militer Amerika Serikat, tentunya perbuatan tersebut diklasifikasikan sebagai perbuatan melanggar hukum dengan Unsur kesalahan *(schuldlement)* terlihat jelas dengan pihak Muslimpro yang tidak menjalankan kewajiban hukum untuk menjalankan segala kegiatan elektronik dengan andal dan aman, atas hal tersebut tentu timbul kerugian *(schade)* dimana sebagai suatu perbuatan melanggar hukum kerugian yang dialami oleh pengguna aplikasi tersebut termasuk juga dengan kerugian immateril yakni kerugian berupa rasa takut atas nasib data pribadi yang telah disetor pada aplikasi serta rasa kecewa atas minimnya manajemen pengendalian risiko. Setelah dilakukannya investigasi oleh Motherboard Vice pihak Muslimpro pun memutuskan hubungan kerjasama dengan perusahaan X-Mode.

b. Penulisan pemberitahuan data pribadi pada aplikasi

Penulisan pemberitahuan atas nasib data pribadi pengguna merupakan bagian dari transparansi penyedia aplikasi yang telah diatur oleh negara dengan mengatur adanya prefrensi berupa kebijakan privasi sebagai bagian dari sertifikat keandalan yang bersifat melengkapi sistem elektronik dengan tujuan untuk melindungi pengguna ataukah konsumen, hal tersebut sebagaimana yang diatur dalam Pasal 76 Ayat (1) Huruf C Peraturan Pemerintah No 71 Tahun 2019, Adanya peraturan tersebut menunjukkan adanya perhatian khusus atas transparansi data dalam sistem elektronik oleh negara terlebih-lebih kejelasan atas data pribadi yang digunakan oleh aplikasi meliputi persetujuan pihak pengguna sebagai hak atas data yang dimiliki. Sejalan dengan hal tersebut pihak Google Play Store jugalah mendukung penuh hak pengguna terhadap data pribadinya dengan mewajibkan pencantuman kebijakan privasi atau *privacy policy* pada setiap aplikasi yang memerlukan data pribadi para pengguna yang dituliskan secara jelas data apakah saja yang digunakan seperti identitas, informasi keuangan dan pembayaran, telepon dan kontak, lokasi perangkat, *short message service* (SMS) maupun data terkit panggilan serta akses pada mikrofon maupun kamera, dimana pada umumnya jenis aplikasi yang memerlukan data tersebut ialah aplikasi jual beli (*e-commerce*), media sosial, dan jasa keuangan (*fintech)*. Kebijakan privasi yang ditulis tersebut jugalah harus memuat secara jelas data apakah saja yang digunakan serta menuliskan pihak ketiga jika melibatkan pihak lain (Kebijakan Program Developer Google Play Store, 2021).

Transparansi data pribadi dalam aplikasi meskipun telah diatur oleh negara maupun pihak privat yakni Google Play Store dalam praktiknya masih belum optimal, dimana masih ditemukan adanya tindakan perbuatan melanggar hukum dengan tidak ditemukannya komitmen penulisan atas data pribadi pengguna baik dalam bentuk *privacy policy* maupun *terms and conditions* pada beberapa aplikasi, salah satunya yakni aplikasi jual-beli BeautyHaul yang telah diunduh lebih dari 10.000 kali, dimana aplikasi tersebut tidak memberikan kepastian atas nasib data pribadi yang diminta oleh aplikasi seperti identitas, nomor telepon, akses lokasi dan detail transaksi pembayaran (Laman Beautyhaul, 2021). Keenggangan beberapa aplikasi untuk menjadi lebih transparan atas data pribadi penggunanya sungguh amat disayangkan, hal ini

dikarenakan praktik penggunaan *privacy policy* bagi bisnis maupun organisasi publik ataukah swasta praktis untuk dilakukan, tidak perlu menunggu dorongan dari pemerintah untuk menampilkan kebijakan privasi dihalaman beranda situs ataukah aplikasi dikarenakan *OECD (Organisation for Economic Co-operation and Development)* telah memberikan alat dalam bentuk situs yang dapat mempermudah bagi pihak-pihak yang berkepentingan untuk membuat *privacy policy*-nya sendiri (OECD, 2003).

c. Cacat administrasi penyediaan aplikasi

Penyediaan suatu aplikasi sebagai sistem elektronik yang dapat diakses masyarakat sejatinya telah diatur oleh pemerintah dengan cara didaftarkan terlebih dahulu kepada kementerian komunikasi dan informatika melalui perizinan berusaha terintegrasi secara elektronik (PBTSE) ataukah juga disebut dengan *online single submission* (OSS), hal tersebut sebagaimana apa yang tercantum dalam Pasal 6 Ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Pasal 5 Peraturan Menteri Nomor 36 Tahun 2014 Tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik junctis Pasal 2 Peraturan Menteri Nomor 7 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika.

Selain itu dalam menyelenggarakan aplikasi penyelenggara sistem elektronik baik lingkup publik maupun privat berdasarkan Pasal 23 Peraturan Pemerintah Nomor 71 Tahun 2019 diwajibkan untuk melakukan pengamanan terhadap sistem komponen elektronik yang diwujudkan dengan kewajiban menggunakan sertifikat elektronik dan disarankan memiliki sertifikat keandalan seperti yang dimuat dalam Pasal 42 Peraturan Pemerintah Nomor 71 Tahun 2019. Sertifikat elektronik tersebut harus didapatkan melalui penyelenggara sertifikasi di Indonesia, yang dimana sampai bulan Juli 2021 terdapat 7 perusahaan penyelenggara sertifikasi elektronik di Indonesia yakni PrivyID, Perum Peruri, Vida, Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara, DigiSig, Badan Pengkajian dan Penerapan Teknologi (BPPT), serta PT Djelas Tanda Tangan Bersama (Informatika, 2021).

Kendati demikian masih terdapat aplikasi yang belum terdaftar dalam sistem OSS yang tentunya menyebabkan kurangnya pemantauan dari pihak pemerintah sehingga memperbesar resiko terhadap keamanan aplikasi, salah satu aplikasi yang belum terdaftar ialah aplikasi kredit secara daring yakni Kredit Impian yang dapat ditemukan dalam layanan Google Play Store. Aplikasi Kredit Impian tersebut sampai dengan bulan Juni 2021 tidak didaftarkan secara resmi berdasarkan penelusuran penulis melalui situs OJK (Jasa Keuangan, 2021) yang menunjukan bahwa aplikasi tersebut tidak terdaftar sebagai salah satu dari 125 *peer to peer lending* yang terdaftar dari total 1.679 penyelenggara sistem elektronik (PSE) yang terdaftar pada laman situs Direktorat Tata Kelola Aplikasi Informatika (Tata Kelola Aptika, 2021).

3.2 Bentuk Upaya Penyelesaian Sengketa Bagi Pengguna Aplikasi pada Google Play Store yang Mengalami Penyalahgunaan Data Pribadi

Kegiatan berbasis sistem elektronik yang melibatkan dua pihak ataukah lebih tentunya memiliki potensi terjadinya sengketa dikarenakan salah satu pihak tersebut tidak menjalankan sesuai perjanjian yang disepakati (wanprestasi) ataukah pihak tersebut melakukan perbuatan yang merugikan orang lain (perbuatan melanggar hukum). Sebagaimana diketahui bentuk-bentuk perbuatan melanggar hukum berkaitan data pribadi dapatlah berupa keamanan sistem aplikasi, transparansi pihak pembuat aplikasi dalam mengolah data serta cacat administrasi pembuatan aplikasi, dimana hal tersebut menitikberatkan pihak yang patut digugat dalam

tindakan terkait penyalahgunaan data pribadi pengguna yakni pihak pengembang ataukah *developer* aplikasi tersebut.

Gugatan terhadap pemilik aplikasi termasuk dalam upaya penyelesaian sengketa dengan sistem litigasi yakni proses penyelesaian sengketa melalui jalur pengadilan, dimana pada kasus-kasus bermuatan penyalahgunaan data pribadi akibat sistem elektronik yang menyebabkan kerugian dapat dilayangkan menggunakan gugatan perbuatan melanggar hukum baik oleh pihak perorangan maupun secara perwakilan sesuai dengan Pasal 38 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Gugatan perbuatan melanggar hukum sendiri merupakan gugatan yang masuk dalam golongan gugatan ke-I yakni gugatan bersifat perseorangan dari ke-III golongan gugatan yang dikenal dalam hukum perdata antara lain gugatan bersifat perseorangan *(persoonlijke rechtsvordering*), gugatan bersifat kebendaan *(zakelijke rechtsvordering)* dan gugatan bersifat campuran *(gemengde rechtsvordering)* (Prodjodikoro, 2018). Perbuatan penyalahgunaan data pribadi tersebut masuk pada golongan gugatan yang bersifat perseorangan berdasarkan peraturan perundang-undangan berupa Pasal 1365 Kitab Undang-Undang Hukum Perdata yang memberi penekanan bahwa setiap pihak yang melakukan perbuatan melanggar hukum wajib untuk mengganti kerugian, serta berdasarkan ketentuan Pasal 21 Ayat (2) Undang-Undang No 11 Tahun 2008 Tentang ITE yang menyatakan bahwa segala akibat hukum menjadi tanggung jawab penyelenggara agen elektronik jika dilakukan melalui agen elektronik tersebut.

Peristiwa gugatan perbuatan melanggar hukum atas data pribadi telah ditempuh oleh para pengguna aplikasi, salah satunya ialah gugatan yang dilayangkan pada aplikasi Tokopedia dengan Komunitas Konsumen Indonesia (KKI) sebagai penggugat dan Menteri Komunikasi dan Informatika Republik Indonesia sebagai Tergugat I maupun Tokopedia sebagai Tergugat II dengan nomor gugatan 235/Pdt.G/2020/PN Jkt.Pst. Gugatan tersebut dibuat dikarenakan para pengguna aplikasi Tokopedia mengalami kerugian atas data pribadinya yang bocor, dimana terdapat 91 juta data pribadi pengguna aplikasi Tokopedia yang bocor sehingga menimbulkan keresahan bagi para pengguna serta masyarakat, kasus tersebut jugalah tepat untuk ditangani menggunakan jalur litigasi gugatan perbuatan melanggar hukum, dimana terdapat pihak Komunitas Konsumen Indonesia (KKI) yang secara sah mewakili para pengguna Tokopedia untuk menggugat dengan dasar Pasal 38 Ayat (2) Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kasus jual-beli data seperti Tokopedia selain menggunakan jalur gugatan perdata juga dapat dilihat dari sisi pidana dimana perbuatan penerobosan data yang dilakukan oleh *hacker* atas aplikasi Tokopedia tersebut melanggar Pasal 32 Ayat (2) Undang-Undang tentang Informasi dan Transaksi Elektronik No 11 Tahun 2008 berupa kegiatan pemindahan informasi elektronik dengan sengaja ataukah melawan hukum kepada pihak yang tidak berhak. Kegiatan yang menimpa aplikasi Tokopedia tersebut mengandung unsur kesalahan baiklah sengaja ataukah tidak (lalai) yang disematkan kepada aplikasi Tokopedia, hal tersebut termasuk kedalam tindakan kejahatan tanpa sepengetahuan pemilik sistem elektronik Tokopedia dan dapat dikenakan sanksi pidana penjara paling lama 9 bulan dan ataukah denda dengan nominal paling banyak Rp. 3.000.000.000,- (tiga miliar rupiah) berdasarkan Pasal 48 Ayat (2) Undang-Undang A Quo. Berdasarkan kasus tersebut dapat dinilai bahwa pihak Tokopedia memenuhi unsur kesalahan dengan tidak memiliki sistem keamanan yang baik dalam aplikasinya sementara pihak tersebut meminta banyak data pribadi termasuk identitas pribadi serta detail pembayaran untuk transaksi jual-beli secara daring yang mengakibatkan timbulnya rasa kekecewaan dan ketakutan atas nasib data pribadi pengguna aplikasi (Franedya, 2021)

Mekanisme penyelesaian sengketa yang terjadi atas peristiwa perbuatan melanggar hukum berkaitan data pribadi tersebut tidak hanya terbatas melalui jalur litigasi dengan gugatan perdata saja, melainkan juga dengan jalur alternatif penyelesaian sengketa ataukah (APS) yang umumnya

lebih disukai oleh pihak penyelenggara aplikasi dikarenakan mengedepankan unsur *win-win solution* yakni solusi yang sama-sama menguntungkan bagi kedua belah pihak dimana pihak penyelenggara sistem elektronik dapat bertanggung jawab tanpa dibebankan beban berat serta rasa malu, dan pihak pengguna mendapatkan kompensasi yang disepakati, hal ini sejalan dengan amanat Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 39 Ayat (2) yang memberikan opsi penggunaan APS sebagai upaya penyelesaian sengketa. Perkembangan teknologi yang masif dengan umunya teknologi informasi turut mengembangkan APS dengan terciptanya penyelesaian sengketa secara online atau acap diistilahkan sebagai *Online Dispute Resolution* (ODR) (Sitompul, Syaifuddin, and Yahanan, 2016).

ODR merupakan bagian daripada alternatif penyelesaian sengketa maka cangkupan penyelesaian sengketanya jugalah sesuai dengan apa yang telah diakui oleh negara dalam Pasal 1 Angka 10 Undang-Undang No 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa yakni berupa Konsultasi, negosiasi, mediasi, konsiliasi, penilaian ahli, serta arbitrase dimana ke-enam pilihan tersebut berfungsi sebagai sarana penyelesaian sengketa yang sah dilakukan untuk menjembatani permasalahan agar dapat selesai di luar koridor persidangan (non-litigasi). Praktik penyelesaian sengketa mengenai data pribadi suatu aplikasi secara non litigasi dapat diselesaikan hanya dengan melibatkan kedua belah pihak yakni pengguna dan pembuat aplikasi ataukah melibatkan pihak ketiga yakni Google Play Store sebagai pihak penyedia distribusi aplikasi ataupun mediator. Cara negosiasi umum dilakukan dan menjadi pilihan yang cukup jamak dipilih sebagai mekanisme penylesaian sengketa non-litigasi oleh para pihak, hal ini dengan cara pengguna aplikasi yang merasa hak atas kemanan data pribadinya tidak terjamin dapat meminta kejelasan ataukah klarifikasi atas permasalahan tersebut dan melangsungkan komunikasi dua arah untuk menyelesaikan permasalahan seperti kompensasi maupun jaminan dengan bukti nyata yang disepakati melalui media email ataukah call center pada aplikasi terkait.

Negosiasi selain dapat dimulai oleh pengguna jugalah dapat diinisiasi oleh pembuat aplikasi dengan cara membuka kesempatan bagi para pengguna untuk memanfaatkan layanan bertanya secara gratis yang diumumkan melalui email pemberitahuan sebagaimana yang dilakukan oleh aplikasi Shopback yang sempat mengalami kejadian pembobolan data pada sistem aplikasinya (Koh and Chong, 2020), pemberitahuan tersebut dibuat sebagai bentuk klarifikasi atas peristiwa pembobolan data terkait keamanan sistem sekaligus membuka pintu bagi para pengguna untuk dapat berkomunikasi dengan harapan adanya kesempatan tersebut para pihak dapat berkomunikasi secara lebih intens dan mencapai solusi terbaik.

Sedang Google Play Store sebagai layanan distribusi aplikasi buatan para pengembang aplikasi juga turut adil dalam membantu penyelesaian sengketa dengan menyediakan fasilitas ODR yang dimana pihaknya memfasilitasi adanya mekanisme penyelesaian sengketa melalui cara mediasi maupun mekanisme laporkan aplikasi yang menyalahi peraturan kebijakan pengembang program ataukah perjanjian distribusi pengembang. Prosedur mediasi dilangsungkan Google Play Store bersama dengan mediator yang disepakati dan bersifat sukarela tanpa adanya paksaan, oleh karenanya kedua belah pihak yang bersengketa maupun Google Play Store tidak berkewajiban untuk menyelesaikan sengketa melalui mediasi.

Sayangnya prosedur mediasi hanya dapat disediakan pihak Google Play Store untuk para pengembangaplikasi yang berdomisili di negara uni eropa saja dan mengedarkan jasa maupun produknya di negara uni eropa dikarenakan merujuk pada Peraturan Uni Eropa 2019/1150 tentang mempromosikan keadilan dan transparansi bagi pengguna bisnis layanan perantara online, sementara mekanisme melaporkan aplikasi dapat dilakukan oleh para pengguna aplikasi di seluruh dunia jikalau menemukan adanya pelanggaran yang dilakukan oleh pihak aplikasi dikarenakan melakukan pelanggaran hukum ataupun melanggar hak pengguna dengan

menandai *(flag)* terlebih dahulu aplikasi sebelumnya *(*Pembaharuan dan Referensi Lainnya Google Play Store, 2021).

3.3 Tanggung Jawab Hukum Google Play Store

Peristiwa perbuatan melanggar hukum terkait data pribadi acap dilakukan oleh pihak *developer* apliaksi sehingga sangat jelas pihak tersebut bertanggung jawab atas perbuatannya, namun begitu pihak Google Play Store sebagai pihak penyedia layanan berbagai macam aplikasi meskipun tidak melakukan perbuatan melanggar hukum terkait penyalahgunaan data pribadi sejatinya telah melakukan kelalaian jika diketahui bahwa aplikasi didalamnya terbukti melakukan perbuatan melanggar hukum, faktor kelalaian tersebutlah yang mengikat Google Play Store untuk dapat bertanggung jawab sebagaimana yang dikehendaki dalam ketentuan Pasal 1366 Kitab Undang-Undang Hukum Perdata.

Konsep tanggung jawab hukum merupakan implikasi dari prinsip kehati-hatian yang ada dalam pelaksanaan kegiatan melalui media elektronik sesuai dengan penjelasan Pasal 3 Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu tiap pihak yang berada didalamnya dituntut untuk selalu memperhatikan dan menimbang setiap aspek yang berpotensi mengakibatkan kerugian bagi pihak lain. Dimana tanggung jawab hukum ialah pertanggung jawaban yang melekat pada setiap orang atas kerugian.yang dialami oleh pihak yang mengalami kerugian diman pertanggung jawaban tersebut fokus kepada aspek pemulihan dan usaha pencegahan, tanggung jawab tersebut dikategorikan dalam 2 (dua) jenis yakni tanggung jawab sebelum terjadinya suatu kejadian (*ex-ante liability*) yang dilakukan dengan cara memberikan regulasi keamanan ataupun standar kualitas pelayanan dengan tujuan untuk mematuhi hukum yang berlaku dan memberi materi yang memadai bagi pihak terkait, serta jenis ke-dua yakni tanggung jawab setelah kejadian (*ex-post liability*) berupa pemberian kompensasi atas kerugian yang telah dialami oleh pihak terkait agar dapat meminimalisir kerugian yang terjadi dengan harapan keadaan dapat pulih seperti semula (Widjawan, 2017).

Tanggung jawab hukum Google Play Store atas data pribadi pengguna sebelum terjadinya suatu kejadian *(ex-ante liability)* dapat dilihat dari isi perjanjian yang mengikat pihak *developer* dalam bentuk kebijakan pengembang program *(developer program policy)* serta perjanjian distribusi pengembang *(developer distribution agreement)* meliputi:

1. Komitmen melindungi privasi pengguna dengan mewajibkan pengembang aplikasi untuk membatasi akses pengumpulan data pribai pengguna sesuai kebutuhan serta menangani data dengan aman;
2. Mewajibkan pengembang aplikasi untuk menampilkan *privacy policy* pada aplikasi yang mengungkap secara eksplisit jenis data pribadi apa sajakah yang diakses serta bagaimana cara aplikasi menangani data pengguna;
3. Menggunakan proses izin akses yang jelas kepada pengguna diikuti dengan tindakan bersifat mengesahkan seperti mengetuk tombol menerima. (Kebijakan Program Developer Google Play Store, 2021)

Regulasi yang diciptakan secara internal oleh Google Play Store berkaitan dengan komitmen pengamanan data juga diikuti dengan tindakan pelaksanaan sanksi yang dilakukan oleh Google Play Store terhadap *developer* aplikasi jika ditemukan pelanggaran yang menyalahi kesepakatan yang disepakati oleh kedua belah pihak, khususnya mengenai penyalahgunaan data pribadi maka akan dilakukan tindakan pertanggung jawaban setelah kejadian terjadi ataukah *ex-post liability* dengan mengaplikasikan 5 (lima) tindakan penegakan hukum sebagaimana bentuk

pertanggung jawaban Google Play Store terhadap pelanggaran tersebut yang dilakukan bertahap, meliputi tindakan pembatasan visibilitas aplikasi dimana *keyword* pencarian nama aplikasi dinon-aktifkan, selanjutnya ialah tindakan penolakan pembaruan aplikasi dimana aplikasi tersebut akan terjebak pada versi lama dan tidak diizinkan untuk memperbarui aplikasinya sebelum memperbaiki kesalahan, selanjutnya penghapusan aplikasi yang dilakukan sementara, dimana aplikasi tidak akan tersedia pada layanan Google Play Store sampai dengan aplikasi tersebut diubah. jika masih dilakukan pelanggaran secara berulang maka akan dilakukan penangguhan *(suspension)* yang dimana aplikasi maupun format berkas pendistribusiannya tidak dapat digunakan. Serta langkah terakhir yang dilakukan jika pelanggaran tersebut dinilai berat dan berulang ialah penghentian akun pengembang aplikasi dimana kedepannya secara otomatis pihak pengembang secara permanen tidak akan disetujui untuk membuat akun kembali meskipun menggunakan akun lain (*Enforcement Process* Google Play Store, 2021).

4. Kesimpulan

Berdasarkan pemaparan diatas maka dapat disimpulkan, bahwa:

1. Perbuatan dapat diklasifikasikan sebagai perbuatan melanggar hukum jika perbuatan tersebut melanggar peraturan perundang-undangan yang berlaku seperti ditemukan aplikasi yang cacat secara administrasi dikarenakan tidak didfatarkan kepada kementerian komunikasi dan informatika melalui perizinan berusaha terintegrasi secara elektronik (PBTSE) sesuai amanat dalam Pasal 2 Peraturan Pemerintah No 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta melanggar kesusilaan, ataukah bertentangan dengan kepentingan orang lain yakni dengan rentannya data pribadi pada aplikasi yang berimbas dengan adanya peristiwa jual beli data pribadi. Selain perbuatan melanggar hukum terhadap data pribadi juga berkaitan dengan transparansi pengembang aplikasi mengenai penulisan pemberitahuan status data pribadi yang tidak dituliskan dalam *privacy policy* atau *terms and conditions*.
2. Pengguna aplikasi yang mengalami perbuatan melanggar hukum terkait penyalahgunaan data pribadi dapat menempuh upaya penyelesaian sengketa secara litigasi melalui gugatan perbuatan melanggar hukum melalui pengadilan, ataukah dapat melakukan proses penyelesaian sengketa secara non litigasi diluar pengadilan. Upaya non litigasi dapat dilakukan kepada pihak pengembang aplikasi melalui upaya negosiasi via chat dan e-mail, ataupun kepada pihak Google Play Store dengan cara melaporkan aplikasi yang dianggap telah melanggar peraturan yang nantinya akan ditindak lanjuti oleh Google Play Store dengan pengenaan sanksi yang pantas, mengingat Google Play Store sebagai wadah distribusi aplikasi memiliki beban tanggung jawab hukum terhadap kelalaian, sedangkan kepada pengembang aplikasi dan pengguna yang berdomisili di wilayah Uni Eropa disediakan mekanisme mediasi dengan mediator yang disetujui oleh Google Play Store.

Daftar Referensi

Buku

Dewi, S. (2009). *Cyber Law 1 : Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*. Widya Padjadjaran.

Fuady, M. (2017). *Perbuatan Melawan Hukum Pendekatan Kontemporer*. PT Citra Aditya Bakti.

Karo-Karo, R., & Prasetyo, T. (2020). *Pengaturan Perlindungan Data Pribadi di Indonesia : Perspektif Teori Keadilan Bermartabat*. Penerbit Nusa Media.

Munir, N. (2017). *Pengantar Hukum Siber Indonesia*. PT Raja Grafindo Persada.

OECD. (2003). *Privacy Online : OECD Guidance on Policy and Practice* (OECD (Ed.)). OECD Publications.

Priowirjanto, E. S. (2019). *Trustmark Sebagai Jaminan Perlindungan Bagi Konsumen Internet Banking di Indonesia*. Keni Media.

Prodjodikoro, W. (2018). *Perbuatan Melanggar Hukum Dipandang Dari Sudut Hukum Perdata*. CV Mandar Maju.

Waluyo, B. (2008). *Penelitian Hukum dalam Praktek*. Sinar Grafika.

Widjawan, D. (2017). *E-Logistic Contract : Tanggung Jawab Pelaku Usaha Terhadap Malfunction, Keamanan Siber, dan Data Pribadi*. Keni Media.

Artikel Jurnal

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia : Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 370. https://doi.org/https://doi.org/10.24815/kanun.v20i2.11159

Sitompul, G., Syaifuddin, M., & Yahanan, A. (2016). Online Dispute Resolution (ODR): Prospek Penyelesaian Sengketa E-Commerce di Indonesia. *Renaissance*, *1*(2), 75. http://www.ejournal-academia.org/index.php/renaissance/article/view/15

Artikel Internet

Clinten, B. (2020). *Data Pengguna Aplikasi Pinjaman Online Cermati.com Disebut Bocor dan Dijual di Internet*. https://tekno.kompas.com/read/2020/11/02/08050067/

Cox, J. (2020). *How the U.S. Military Buys Location Data from Ordinary Apps*. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x?fbclid=IwAR0mDyXT44VS5jrJcdo1rYJKdb0nmvPJQRJrh_PEkIMLxUAif_dmvNbGXyw.

Criddle, C. (2020). *Facebook sued over Cambridge Analytica data scandal*. https://www.bbc.com/news/technology-54722362

Enforcement Process Google Play Store. (2021). https://support.google.com/googleplay/android-developer/answer/9899234?hl=en

Franedya, Roy. 2021. "91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M." https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m.

Jasa Keuangan, O. (2021). *Penyelenggara Fintech Lending Terdaftar dan Berizin di OJK per 10 Juni 2021*.https://www.ojk.go.id/id/kanal/iknb/financial-technology/Pages/Penyelenggara-Fintech-Lending-Terdaftar-dan-Berizin-di-OJK-per-10-Juni-2021.aspx

Kebijakan Program Developer Google Play Store. (2021). https://support.google.com/googleplay/androiddeveloper/answer/10477564?hl=id&ref_topic=9877065

Kementrian Komunikasi dan Informatika Republik Indonesia. (2021). *Status Pengakuan Penyelenggara Sertifikasi Elektronik*. https://tte.kominfo.go.id/listPSrE/_

Kemp, S. (2021). *Digital 2021 : Indonesia*. https://datareportal.com/reports/digital-2021-indonesia

Koh, F., & Chong, C. (2020). *ShopBack and RedDoorz Report Data Bbreaches*. https://www.thejakartapost.com/life/2020/09/27/shopback-and-reddoorz-report-data-breaches.html,

Laman *Beautyhaul*. (2021). https://play.google.com/store/apps/details?id=com.beautyhaul.beautyhaul

Perjanjian Distribusi *Developer Google Play*. (2020). https://play.google.com/about/developer-distribution-agreement/archive.html.

Tata Kelola Aptika, D. (2021). *Daftar Penyelenggara Sistem Elektronik*. https://pse.kominfo.go.id/tdpse-terdaftar

Pembaharuan dan Referensi Lainnya Google Play Store. (2021). https://support.google.com/googleplay/android-developer/topic/9877065

PeraturanPerundang-Undangan

Kitab Undang-Undang Hukum Perdata

Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika

Peraturan Menteri Komuikasi dan InformatikaNomor 36 Tahun 2014 Tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-UndangNomor 30 Tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa