URGENSI UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL

Oleh:

Putu Sekarwangi Saraswati[1], I Nengah Susrama[2]
Fakultas Hukum Universitas Mahasaraswati, Email: sekarwangisaraswati@gmail.com

ABSTRAK

Undang-Undang Data Pribadi akan menjadi payung bagi aturan-aturan yang bermacam-macam ini. Tujuannya untuk mengharmonisasi aturan data priabadi dan menghindari tumpang tindih aturan. Selain itu Undang-Undang data pribadi juga diperlukan untuk mengatur isu-isu terbaru seperti big data dan anonymisation. Pentingnya payung hukum privasi data menjadi salah satu wacana yang bergulir di era digital ini. Pasalnya, kebocoran dan jual beli data ilegal marak terjadi dan diperdagangkan oleh oknum. Terutama pencurian data di *e-commerce*. Regulasi Undang-Undang Perlindungan Data Pribadi memberikan landasan hukum bagi bangsa Indonesia, untuk menjaga kedaulatan negara, keamanan negara, dan perlindungan terhadap data pribadi milik warga negara Indonesia, di manapun data pribadi tersebut berada. Tanpa regulasi perlindungan data pribadi,bangsa Indonesia akan kehilangan peluang sosial ekonomi.Bahkan keamanan negara terancam, karena data pribadi merupakan komoditas bisnis dan kerahasiaan warga negara, paparnya pada Alinea Forum bertajuk Menanti Ketegasan Komitmen Menjaga Keamanan Data Pribadi.

Kata Kunci : Payung Hukum, Perlindungan, Data Pribadi, Era Digital.

ABSTRACT

The Personal Data Law will serve as an umbrella for these various regulations. The goal is to harmonize private data rules and avoid overlapping rules. Apart from that, the personal data law is also needed to regulate the latest issues such as big data and anonymization. The importance of a data privacy legal umbrella is one of the discourses that are rolling in this digital era. This is because leaks and buying and selling of illegal data are rife and trafficked by unscrupulous individuals. Especially data theft in e-commerce. The regulation of the Personal Data Protection Act provides a legal basis for the Indonesian nation, to safeguard state sovereignty, state security, and protection of personal data belonging to Indonesian citizens, wherever such personal data is located. Without regulations on personal data protection, the Indonesian nation will lose socio-economic opportunities. Even state security is threatened, because personal data is a business commodity and citizen confidentiality, he explained in the paragraph forum entitled Waiting for Firm Commitment to Maintain Personal Data Security.

Key Word: The Regulation, Protection, A Data Privacy, Digital Era.

I. Pendahuluan

1.1 Latar Belakang Masalah

Kemajuan teknologi dan informatika di era digital ini sangat cepat bahkan hampir semua sektor publik maupun bisnis memakai sistem teknologi berbasis online untuk memudahkan dalam melakukan aktivitas pelayanan serta berbagai informasi yang dibutuhkan oleh masyarakat maupun konsumen suatu perusahaan.

Tentu saja setiap kemajuan pasti mempunyai dampak buruk yang meningkatkan resiko terjadinya tindak kejahatan, terutama yang belakangan marak misalnya penyalahgunaan informasi data diri. Salah satu contoh kasus menarik perhatian masyarakat adalah penyalahgunaan Nomor Induk Kependudukan (NIK) dan Kartu Keluarga (KK) dalam registrasi kartu SIM untuk telepon genggam yang menimpa seorang penggiat media sosial bernama deni siregar yang memang aktif di media sosial yang sering mengangkat isu radikalisme di Indonesia, data diri termasuk alamat lengkapnya dicuri oleh salah satu pegawai provider telekomunikasi tempat yang bersangkutan mendaftarkan registrasi kartu SIM berdasarkan NIK dan KK. Data itu kemudian disebarkan oleh oknum provider sehingga beberapa waktu yang lalu rumahnya didatangi oleh beberapa orang dan keluarga dirumah mengalami intimidasi serta ancaman dari orang-orang tersebut. Kasusnya saat ini masih dalam penyelidikan pihak kepolisian.

Pada 2019, hampir 80% orang Indonesia rentan menjadi korban kejahatan di dunia maya . Salah satu penyebabnya adalah belum adanya kesadaran dari pengguna internet di Indonesia untuk melindungi data pribadi mereka. Penelitian dari Asosiasi Penyelenggara Jasa Internet Indonesia menunjukkan 92% dari responden mereka dengan mudah memasukkan informasi data pribadi berupa nama ke aplikasi di internet, lalu 79% memberikan informasi tentang tempat dan tanggal lahir mereka, bahkan 65% memberikan alamat pribadi.[1]

Informasi tentang data diri ini sangatlah penting untuk dilindungi karena memuat banyak sekali informasi terkait seseorang, mulai data diri, data keuangan, riwayat perjalanan sampai riwayat kesehatan. Beberapa kasus yang terjadi diakibatkan kurang efektifnya peraturan maupun UU tentang perlindungan data diri disamping memang belum adanya UU khusus yang memayungi hal tersebut. Beberapa Undang-Undang yang membahas terkait perlindungan data diri tersebar ke beberapa Undang-Undang dan Peraturan setingkat Menteri. Hal inilah yang mendorong penulis untuk membuat sebuah kajian terkait urgensi segera disahkannya UU tentang Perlindungan Data Diri yang saat ini masih dalam bentuk Rancangan Undang-Undang untuk segera ditindaklanjuti oleh Pemerintah dan DPR.

1.2 Rumusan Masalah

1. Mengapa UU Perlindungan Data Pribadi sangat penting untuk segera disahkan?

II. Metode Penelitian

2.1 Jenis Penelitian

Penelitian ini menggunakan metode normatif atau penelitian

[1]Faiz Rahman, Annisa Rahma Diasti,2020, ***Bagaimana mewujudkan UU Perlindungan Data Pribadi yang kuat di Indonesia,*** **Artikel Fakultas Hukum Universitas Gadjah Mada, Yogjakarta.**

perpustakaan, merupakan penelitian yang mengkaji studi dokumen, yaitu menggunakan data sekunder seperti peraturan perundang-undangan maupun pendapat para sarjana.

2.2 Sumber Bahan Hukum

Penelitian menggunakan Metode Penelitian Normatif. Penelitian hukum normatif menggunakan bahan hukum primer, sekunder, dan tersier mencakup :

a. Data primer sebagai data utama yaitu UUD 1945 terutama Pasal 28G ayat (1) yang berbunyi "Setiap orang berhak atas perlindungan diri pribadi, keluarga, dan kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".
b. Bahan Hukum Sekunder yaitu bahan hukum yang dapat memberikan penjelasan terhadap bahan hukum primer, yang dapat berupa rancangan peraturan Perundang - Undangan, hasil penelitian, buku-buku teks, jurnal ilmiah, surat kabar koran), brosur, dan berita internet, serta webinar dengan narasumber dan tema yang sesuai dengan judul penelitian. Terkait penelitian ini maka digunakan sumber dari kepustakaan seperti buku-buku yang berkaitan dengan masalah yang dibahas, yaitu mengenai Pentingnya Perlindungan data pribadi.
c. Bahan Hukum Tersier adalah bahan non hukum yang digunakan untuk menjelaskan, baik bahan hukum primer maupun bahan hukum sekunder, seperti kamus, ensiklopedi, leksikon, dan lain-lain."

2.3 Teknik Pengumpulan Bahan Hukum

Studi Pustaka dengan menelaah terhadap peraturan perundang-undangan buku, majalah ilmiah, jurnal, hasil penelitian sebelumnya, artikel, index, maupun ensiklopedia yang berhubungan dengan materi yang diteliti.

III. Pembahasan

3.1 Pengertian dan Pentingnya Perlindungan Terhadap Data Pribadi

Saat ini data pribadi merupakan sesuatu yang sangat penting untuk dilindungi serta dijaga kerahasiaannya dari pihak lain, karena ada banyak sekali tindak kejahatan yang terjadi jika data diri disalahgunakan oleh orang yang tidak bertanggung jawab. Hal ini sejalan dengan perkembangan teknologi dan informatika pada saat ini yang berkembang sangat pesat. Teknologi dan informasi menjadi kebutuhan bagi masyarakat pada saat ini. Secara alamiah, manusia tidak mungkin dilepaskan dari kemajuan teknologi yang tujuannya adalah untuk memudahkan kehidupannya. Secara alamiah pula, manusia tidak mungkin dilepaskan dari hukum yang tujuannya adalah untuk menjaga eksistensi.[2] Perkembangan teknologi dan informasi telah mengubah dunia menjadi tanpa batas dan terjadi perubahan sosial yang sangat cepat dan menimbulkan pengaruh negatif yang tidak kalah banyak dengan manfaat yang ada. Pengaruh tersebut bisa dirasakan saat ini adalah dengan mudahnya akses

[2]Edmon Makarim, 2003, *kompilasi hukum telematika*, Raja Grafindo Persada, hlm.7, Jakarta.

teknlogi dan informasi membuat peluang kejahatan yang muncul semakin banyak. Bukan saja kejahatan konvensional seperti pencurian dan penipuan tetapi saat ini yang banyak muncul adalah kasus kejahatan *online* atau disebut juga kejahatan mayantara (*cibercrime*).[3]

Menurut Widodo kejahatan mayantara (*cybercrime*) dengan *internet crime* tidak sama. Pengertian kejahatan *cybercrime* dengan *computer-related crime* adalah sama, jika dalam *cybercrime*, kejahatan dapat dilakukan baik menggunakan internet atau tidak. Dalam kejahatan *cybercrime*, kejahatan dapat dilakukan dengan cara menggunakan komputer yang tidak terkoneksi internet (*offline*), misalnya seseorang yang menggadankan film dalam DVD secara ilegal tidak harus menggunakan internet, tetapi cukup menggunakan data yang sudah ada pada file atau folder di komputer kemudian dicopy pada kepingan DVD. Sedangkan pengertian "kejahatan di Internet", semua kejahatan tersebut dilakukan dalam kondisi komputer terkoneksi dengan sistem internet (*online*). Namun demikian, kejahatan *cybercrime* dengan kejahatan di internet sama-sama menggunakan komputer sebagai basis kejahatan. Dengan demikian, dapat dipahami bahwa kejahatan di internet (*internet crime*) selalu merupakan *cybercrime*, sedangkan *cybercrime* tidak selalu terjadi didalam atau menggunakan internet.[4]

Sejak 1 Desember 2016, Indonesia memiliki peraturan tentang perlindungan data pribadi dalam sistem elektronik. Tertuang dalam Peraturan Menkominfo No. 20 Tahun 2016, dalam Pasal 1 butir 1 dan 2 dijelaskan tentang pengertian dari data diri sebagai bagian dari data perseorangan yang berbunyi :

1) Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.
2) Data perseorangan tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan

Terkait dengan upaya perlindungan data diri dalam sistem elektronik dijelaskan di Pasal 2 yang berbunyi :

1) Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi.
2) Dalam melaksanakan ketentuan sebagaimana dimaksud dalam pada ayat (1) harus berdasarkan asas perlindungan Data Pribadi yang baik, yang meliputi :
    a. Penghormatan terhadap Data Pribadi sebagai privasi;
    b. Data pribadi bersifat rahasia sesuai Persetujuan dan/atau

[3]Andi hamzah, 1990, *Aspek-aspek pidana di bidang komputer*, Sinar Grafika, hlm 23, Jakarta.

[4]Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, hlm.8, Jakarta.

berdasarkan ketentuan Perundang-Undangan;
c. Berdasarkan Persetujuan;
d. Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan;
e. Kelaikan Sistem Elektronik yang digunakan;
f. Itikad baik untuk segera memberitahukan secara tertulis kepada pemilik Data Pribadi atas setiap kegagalan Perlindungan Data Pribadi;
g. Ketersediaan aturan internal pengelolaan perlindungan Data Pribadi;
h. Tanggung jawab atas Data Pribadi yang berada dalam penguasaan pengguna;
i. Kemudahan akses dan koreksi terhadap Data Pribadi oleh pemilik Data Pribadi; dan
j. Keutuhan, akurasi, dan keabsahan serta kemuktahiran Data Pribadi.[5]

3.2 Rancangan Undang - Undang terkait Perlindungan Data Pribadi

Salah satu upaya yang dapat dilakukan untuk memperkuat kerangka hukum perlindungan data pribadi adalah dengan membuat sistem perlindungan yang menerapkan prinsip yang menjunjung perlindungan privasi pengguna dalam tataran regulasi maupun teknis. Prinsip tersebut dipakai dalam pembuatan setiap sistem layanan online dan akan menutup kemungkinan adanya perpindahan kontrol atas data milik pribadi ke sistem. Prinsip ini telah diterapkan negara-negara Uni Eropa dalam aturan perlindungan data pribadi mereka yang dikenal dengan sebutan GDPR (*General Data Protection Regulation*).

Tujuh prinsip itu antara lain dengan tujuan menjunjung tinggi perlindungan privasi pengguna yang memiliki tujuh prinsip utama, yaitu:

1. **Proaktif, bukan reaktif.** Artinya prinsip ini fokus pada antisipasi dan pencegahan.
2. **Mengutamakan privasi pengguna.** Prinsip ini memetakan pada upaya untuk memberikan perlindungan privasi secara maksimum dengan memastikan bahwa data pribadi secara otomatis dilindungi dalam sistem IT atau praktik bisnis tertentu.
3. **Perlindungan privasi diintegrasikan ke dalam desain.** Kewajiban menanamkan perlindungan data pribadi pada desain teknologi secara holistik.
4. **Memiliki fungsi maksimal.** Prinsip ini menekankan pada penyediaan standar mitigasi risiko untuk sistem elektronik yang kewajibannya tidak semata-mata demi keamanan perusahaan, tapi juga demi privasi dari pemilik data pribadi.

[5]https://www.jdih.kominfo.go.id/produk_hukum/inventaris/2016

5. **Sistem keamanan yang total.** Prinsip ini terwujud dengan memperkuat sistem keamanan dari mula hingga akhir.
6. **Transparansi.** Prinsip ini memastikan praktik bisnis maupun teknologi yang ada beroperasi sesuai aturan yang sudah disepakati dan diungkap ke publik. Penyedia jasa juga harus tunduk pada proses verifikasi yang dilakukan oleh pihak independen.
7. **Menghormati privasi pengguna.** Prinsip paling vital yang diwujudkan dengan memberikan peran aktif bagi pemilik data pribadi untuk mengelola data mereka.[6]

Hukum dan teknologi berkembang secara bersama-sama, namun pada kenyataannya tidak dapat dipungkiri bahwa hukum berjalan lebih lambat dibandingkan dengan perkembangan teknologi yang selalu berubah dengan cepat. Ketidakseimbangan antara hukum dan teknologi mengakibatkan perbuatan yang melanggar hukum seperti kejahatan dengan memanfaatkan media telekomunikasi seperti telepon seluler.[7]

Dalam hukum di Indonesia terkait pelindungi data pribadi pengguna internet, pemerintah Indonesia menggunakan beberapa instrumen hukum yang masing-masing berdiri sendiri dan terpisah-pisah antara lain UU tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, dan Peraturan Otoritas Jasa Keuangan (OJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.

Secara umum, ketujuh prinsip di atas sudah ditemukan tersebar pada level peraturan teknis di Indonesia. Misalnya, untuk prinsip proaktif bukan reaktif, Pasal 15 dan Pasal 16 UU ITE mengatur bahwa penyedia sistem elektronik harus menyediakan sistem elektronik yang andal dan aman, dan bertanggung jawab atas operasi sistem, dan menetapkan persyaratan minimum untuk penerapan sistem elektronik tersebut. Lalu prinsip penyediaan keamanan yang total bisa ditemukan dalam Pasal 26 huruf a Peraturan OJK yang mewajibkan terjaganya kerahasiaan, integritas, dan ketersediaan data pribadi sejak awal diperoleh hingga dihancurkan. Sayangnya, pengaturan secara holistik mengenai ketujuh prinsip di atas tidak ditemukan pada level UU dan hanya terpecah-pecah dalam aturan-aturan pelaksana yang berbeda-beda.

Padahal, dengan semakin pesatnya perkembangan teknologi dan meningkatnya jumlah pengguna layanan berbasis teknologi di Indonesia, upaya perlindungan data pribadi memerlukan payung hukum yang lebih kuat guna memberikan jaminan terhadap hak masyarakat atas keamanan data pribadinya. Oleh karena itu, diharapkan Rancangan Undang-Undang Perlindungan Data Pribadi yang saat ini sudah masuk dalam tahap pembahasan

[6] Ikhsan Yusda PP,: *Analisis Terhadap Cyber Crime dalam kaitannya dengan Asas Teritotialitas*, Jurnal TEKNOIF,Vol 3 No.1, ISSN: 2338:2724, hlm:45

[7] Muhamad safri, Andi Softan, Winner sitorus, *"Tindak Pidana Pengancaman Melalui Layanan Pesan Singkat"*, Magister Ilmu Hukum Universitas Hasanudin, Vol.5,No.1 (1 Juni 2016), ISSN; 2252-7230,hlm.86

di Dewan Perwakilan Rakyat (DPR) dapat mengakomodasi seluruh tujuh prinsip di atas. Hal ini penting agar dapat menjadi dasar hukum yang matang dalam pelaksanaan perlindungan data pribadi di Indonesia yang lebih baik pada masa yang akan datang.

Pada tanggal 24 Januari 2020 Presiden Joko Widodo telah menandatangani Rancangan Undang-Undang Perlindungan Data Diri Pribadi (RUU PDP). Dan akan segera dibahas oleh DPR setelah selesai pembahasan RUU omnibus law. Berdasarkan draf per Desember 2019, RUU PDP memuat 72 Pasal dan 15 Bab, yang mengatur tentang definisi data pribadi, jenis, hak kepemilikan, pemrosesan, pengecualian, pengendalian dan prosesor, pengiriman, lembaga berwenang yang mengatur data pribadi, serta penyelesaian sengketa. Selain itu, RUU tersebut juga memuat kerja sama internasional hingga sanksi yang dikenakan atas penyalahgunaan data pribadi.

Poin-poin yang dijabarkan dalam RUU PDP tersebut antara lain memuat :

1. Definisi Data Pribadi
   Draf RUU PDP menyebutkan, definisi data pribadi adalah setiap data tentang seseorang, baik yang teridentifikasi dan dapat diidentifikasi tersendiri atau dikombinasikan dengan informasi lainnya, secara langsung maupun tidak langsung melalui sistem elektronik dan nonelektronik.
2. Jenis-jenis data Pribadi
   Ada dua jenis data pribadi, yakni data yang bersifat umum dan spesifik. Data dikategorikan data umum bila melalui akses pelayanan publik atau tercantum dalam identitas resmi. Misalnya nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang harus dikombinasikan sehingga memungkinkan untuk mengidentifikasi seseorang.
3. Penghapusan data pribadi
   Pengendali data pribadi wajib memusnahkan informasi itu jika data sudah tidak memiliki nilai guna lagi atau habis retensinya. Jika pemilik data meminta menghapus maka pengendali harus menghapusnya.
4. Kegagalan perlindungan data pribadi
   Dalam RUU PDP tersebut disebutkan, jika terjadi kegagalan perlindungan terhadap data pribadi, misalnya data bocor kepihak-pihak lain, pengendali wajib menyampaikan pemberitahuan tertulis aling lambat 3x24 jam kepada pemilik data dan menteri atau instansi pengawas. Pengumuman itu memuat data pribadi yang bocor, kapan, kronologinya, serta upaya penanganan dan pemulihannya.
5. Sanksi pidana atas pelanggaran penggunaan data pribadi
   RUU PDP juga mengenakan sanksi atas pelanggaran data pribadi. Pelaku yang mengungkapkan atau menggunakan data pribadi yang bukan miliknya secara melawan hukum akan dikenakan pidana penjara tujuh tahun atau dikenakan denda 70 miliar. Selain dijatuhi pidana pokok, terdakwa juga dapat dijatuhi pidana tambahan berupa perampasan pendapatan dan

harta kekayaan yang diperoleh atau hasil dari tindak pidana.[8]

IV. Kesimpulan dan Saran

4.1 Kesimpulan

RUU PDP merupakan inisiatif pemerintah yang menjadi prioritas untuk dibahas di DPR. Sebelumnya ada 32 undang-undang yang menyinggung pengaturan data pribadi warga negara, salah satunya UU Informasi dan Transaksi Elektronik (ITE). UU ITE diatur lebih lanjut dalam Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi di Dalam Sistem Elektronik. Namun, peraturan tersebut dirasa belum cukup untuk melindungi data pribadi masyarakat dan mengikuti perkembangan teknologi.

Masalah perlindungan data pribadi ini menjadi perhatian mengingat perkembangan teknologi membuat penyalahgunaan data semakin rentan. Dan banyak sekali pihak-pihak memperjual belikan data pribadi demi kepentingan pribadi dan ini sangat merugikan masyarakat.

4.2 Saran

1) Mengingat sangat pentingnya data pribadi khususnya di era kemajuan teknologi seperti saat ini Pemerintah harus segera mungkin mensahkan UU PDP tersebut guna melindungi bagian dari hak asasi masyarakat yang diamanatkan oleh konstitusi.
2) Pengendali data pribadi yang diamanatkan oleh UU nantinya harus melakukan Pengawasan ketat terhadap pihak-pihak yang meminta data pribadi untuk mengakses layanan, seperti provider telekomunikasi sarta perbankan, agar nantinya tidak terjadi kebocoran data yang dapat merugikan masyarakat.

[8] https://katadata.co.id/hariwidowati/digital/5e9a498eada86/diteken-jokowi-ini-poin-poin-ruu-perlindungan-data-pribadi

Daftar Acuan

Buku

Hamzah, Andi, 1990, *Aspek-aspek pidana di bidang komputer*, Sinar Grafika, hlm 23, Jakarta.

Makarim, Edmon, 2003, *kompilasi hukum telematika*, Raja Grafindo Persada, hlm.7, Jakarta.

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, hlm.8, Jakarta.

Jurnal/Artikel

Faiz Rahman, Annisa Rahma Diasti, 2020, ***Bagaimana mewujudkan UU Perlindungan Data Pribadi yang kuat di Indonesia,* Artikel Fakultas Hukum Universitas Gadjah Mada, Yogjakarta.**

Ikhsan Yusda PP,: *Analisis Terhadap Cyber Crime dalam kaitannya dengan Asas Teritotialitas*, Jurnal TEKNOIF,Vol 3 No.1, ISSN: 2338:2724, hlm:45

Muhamad safri, Andi Softan, Winner sitorus, *"Tindak Pidana Pengancaman Melalui Layanan Pesan Singkat"*, Magister Ilmu Hukum Universitas Hasanudin, Vol.5,No.1 (1 Juni 2016), ISSN; 2252-7230,hlm.86

Undang-Undang/Peraturan

UUD Tahun 1945 Pasal 28G ayat (1)

UU ITE Pasal 26 ayat (1) Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE)

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

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

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

Internet

https://www.jdih.kominfo.go.id/produk_hukum/inventaris/2016

https://katadata.co.id/hariwidowati/digital/5e9a498eada86/diteken-jokowi-ini-poin-poin-ruu-perlindungan-data-pribadi