



AKTUAL JUSTICE
JURNAL ILMIAH MAGISTER HUKUM
PASCASARJANA UNIVERSITAS NGURAH RAI

PRINSIP KEHATI-HATIAN DALAM
PENYELENGGARAAN SISTEM ELEKTRONIK
DALAM UPAYA PERLINDUNGAN DATA
PRIBADI DI INDONESIA

Rai Mantili¹, Putu Eka Trisna Dewi²

¹Dosen Fakultas Hukum Universitas Padjadjaran, E-mail : rai@unpad.ac.id

²Dosen Fakultas Hukum Universitas Ngurah Rai, E-mail: trisnadewi.ecak@gmail.com

Abstract

One of the aspects that must be of concern in electronic transaction activities is the aspect of personal data protection so that the personal data of service users is maintained. One of the principles that must be observed by Electronic System Operators in protecting personal data is the principle of prudence. This paper will examine the principles of prudence in the operation of electronic systems in efforts to protect personal data in Indonesia by using normative research methods. In general, it can be seen that the precautionary principle is not explicitly regulated in the formulation of laws and regulations related to Electronic Information and Transactions or Personal Data Protection, but the provisions of the articles therein contain provisions regarding the principle of prudence. The application of the precautionary principle is carried out with the active efforts of electronic system administrators as the party that manages the personal data of service users to ensure data confidentiality and the security of their electronic systems with all efforts to prevent the system from being compromised by third parties. The legal consequence is that if there is a leak of personal data, the electronic system operator is obliged to be responsible civilian by paying compensation on the basis of a lawsuit by the owner of the personal data who has experienced data leakage and / or material or immaterial loss

Keyword: Prudential Principle, Personal Data Protection, Electronic System Operation

Abstrak

Salah satu aspek yang harus menjadi perhatian dalam kegiatan transaksi elektronik adalah aspek perlindungan data pribadi agar data pribadi pengguna layanan tetap terjaga keamanannya. Salah satu prinsip yang harus diperhatikan oleh Penyelenggara Sistem Elektronik dalam perlindungan data pribadi adalah prinsip kehati-hatian. Tulisan ini akan mengkaji terkait prinsip kehati-hatian dalam penyelenggaraan sistem elektronik dalam upaya perlindungan data pribadi di Indonesia dengan menggunakan metode penelitian normatif. Secara umum dapat diketahui bahwa prinsip kehati-hatian secara eksplisit memang tidak diatur dalam rumusan peraturan perundang-undangan terkait dengan Informasi dan Transaksi Elektronik maupun Perlindungan Data Pribadi, namun dalam ketentuan pasal-

pasal didalamnya memuat ketentuan mengenai prinsip kehati-hatian. Penerapan prinsip kehati-hatian dilaksanakan dengan adanya upaya aktif dari penyelenggara sistem elektronik selaku pihak yang mengelola data pribadi pengguna layanan untuk menjamin kerahasiaan data dan keamanan sistem elektroniknya dengan segala upaya untuk mencegah agar sistem tersebut tidak sampai dibobol oleh pihak ketiga. Akibat hukum bilamana terjadi kebocoran data pribadi maka pihak penyelenggara sistem elektronik wajib bertanggung jawab secara keperdataan dengan membayar ganti kerugian atas dasar gugatan oleh pemilik data pribadi yang mengalami kebocoran data dan/atau kerugian secara materiil maupun immateriil.

Keyword : Prinsip Kehati-hatian, Perlindungan Data Pribadi, Penyelenggaraan Sistem Elektronik

1. Pendahuluan

Teknologi Informasi sebagai suatu teknik yang berfungsi untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan /atau menyebarkan suatu informasi menjadi suatu sarana yang dapat terintegrasi dalam berbagai bidang kegiatan manusia. Keberadaan teknologi dalam berbagai bidang kehidupan membantu manusia dilaksanakan dalam suatu sistem elektronik oleh penyelenggara sistem elektronik tersebut. sebagaimana diatur dalam ketentuan Pasal 1 angka 6 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penyelenggaraan sistem elektronik dapat dilakukan oleh penyelenggara negara, orang, badan usaha dan/atau masyarakat.

Kemudahan yang diberikan dengan adanya kemajuan teknologi informasi dalam berbagai bidang di sisi lain juga membawa dampak negatif yakni antara lain adanya kejahatan siber (cyber-crime), kebocoran data pribadi, penyalahgunaan data, dan jual beli data pribadi dalam pasar gelap. Adanya dampak negatif tersebut sudah pasti akan menimbulkan kerugian bagi masyarakat. Namun dengan adanya perkembangan teknologi hal ini juga berdampak pada berkembang kejahatan di dunia maya sehingga adanya kejahatan cyber yang mana tidak sejalan dengan perkembangan aturan. Beberapa permasalahan hukum yang timbul akibat pemanfaatan teknologi informasi yakni dalam bidang : Hak

Kekayaan Intelektual, Perlindungan Konsumen, Perbankan, Privacy, dan Electronic Commerce.¹

Ada beberapa bentuk permasalahan hukum di bidang data pribadi terkait dengan penyalahgunaan data pribadi diantaranya seperti : penjualan data, data profiling, tujuan pemasaran, penelitian, bahkan termasuk pemantauan/spionase. lebih parah lagi penyalahgunaan data pribadi untuk tindak kriminal seperti pembuatan akun palsu, penipuan dalam jaringan, pencucian uang, pasar palsu dan juga transaksi ilegal. Oleh karena itu, diperlukan rangkaian pengamanan dan aturan yang komprehensif berkenaan dengan data pribadi. ² Menurut Djafar Wahyudi dkk, untuk melakukan perlindungan terhadap data pribadi dapat dilakukan dengan dua metode yakni pertama perlindungan dilakukan terhadap fisik data pribadi tersebut dan kedua melalui regulai yang ditujukan untuk memberikan jaminan keamanan terhadap penggunaan data pribadi tersebut. ³ Berkenaan dengan perlindungan data pribadi terdapat subjek hukum yang harus diatur yakni pengelola data pribadi (orang, badan hukum publik atau swasta dan organisasi kemasyarakatan yang melakukan pengelolaan data pribadi) dan pemroses data pribadi (orang, badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang melakukan pemrosesan data pribadi atas nama pengelola data). ⁴

Sebagaimana yang telah disebutkan dalam Undang-Undang ITE bahwa penyelenggara sistem elektronik memiliki kewajiban untuk melindungi data pengguna layanan sistem elektroniknya agar tidak disalahgunakan. Dasar pemikiran adanya kewajiban perlindungan data

¹ Mansur, D. M.A. & Gultom, E. (2009). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung : Refika Aditama, h.132.

² Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*. Vol.20 No.2 Agustus 2018. h. 370

³ Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi di Indonesia. *Jurnal BECOS*. Vol.1 No.1 September 2019. h. 152

⁴ Rosadi, S.D. (2018). Perlindungan Privasi Data Pribadi dalam Era Ekonomi Digital di Indonesia. *VeJ*. Volume 4 Nomor 1. h. 94.

pengguna layanan sistem elektronik oleh penyelenggara sistem elektronik adalah didasarkan pada prinsip kehati-hatian. Sehingga penyelenggara sistem elektronik harus melakukan segala upaya untuk menjamin keamanan sistemnya agar tidak sampai kebobolan sehingga data pribadi yang tersimpan disana tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.

Atas dasar itu dalam tulisan ini akan mengangkat topik mengenai penerapan prinsip kehati-hatian dalam penyelenggaraan sistem elektronik khususnya di bidang e-commerce dan akibat hukum bagi penyelenggara sistem elektronik yang tidak menerapkan prinsip kehati-hatian dalam penyelenggaraan sistem elektronik.

2. Metode Penelitian

Metode penelitian yang digunakan untuk mengkaji tulisan ini menggunakan metode penelitian hukum normatif. Penelitian hukum normatif adalah suatu penelitian hukum yang melihat hukum sebagai suatu tatanan norma yang berkaitan mencakup asas-asas, norma, kaidah dari peraturan perundang-undangan, putusan pengadilan, perjanjian serta doktrin (ajaran)⁵. Tulisan ini juga menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conseptual approach*) dalam rangka mengkaji penerapan prinsip kehati-hatian dalam kegiatan penyelenggaraan sistem elektronik guna memberikan perlindungan terhadap data pribadi.

⁵ Fajar, M & Ahmad Y. (2010). *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar. h. 34.

3. Hasil Dan Pembahasan

A.Penerapan Prinsip Kehati-hatian dalam Penyelenggaraan Sistem Elektronik dalam rangka Perlindungan Data Pribadi Pengguna Layanan

Sistem elektronik memiliki definisi serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Sedangkan Menurut Peraturan Pemerintah no 71 tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan bahwa “Penyelenggara Sistem Elektronik (“PSE”) adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain”. Sebagaimana diatur dalam ketentuan Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik, pemanfaatan teknologi informasi dan transaksi elektronik salah satunya didasarkan atas asas kehati-hatian. Lebih lanjut dalam ketentuan pasal 19 PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik disebutkan bahwa Penyelenggara Sistem Elektronik harus menerapkan tata kelola sistem elektronik yang baik dan akuntabel. Lebih lanjut disebutkan bahwa Penyelenggara sistem elektronik wajib melakukan pengamanan terhadap komponen sistem elektronik.

Adapun cara yang wajib untuk dilaksanakan untuk menjaga keamanan sistem elektronik sebagaimana disebutkan dalam Pasal 23 PP tentang Penyelenggaraan Sistem Elektronik yaitu:

- a. Penyelenggara sistem elektronik wajib menjalankan prosedur dan sarana untuk pengamanan demi menghindari kegagalan dan kerugian.
- b. Sistem pengamanan tersebut wajib mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman serangan yang menimbulkan kegagalan dan kerugian.
- c. Apabila ada kegagalan atau gangguan pada sistem elektronik tersebut maka Penyelenggara Sistem Elektronik wajib mengambankan informasi dan/atau dokumen elektronik dan segera melaporkan pada aparat penegak hukum atau lembaga negara yang melaksanakan urusan pemerintahan di bidang siber.

Penyelenggara sistem elektronik dalam rangka melakukan penerapan asas kehati-hatian dalam pengaturan di Pasal 31 PP No.71 Tahun 2019 juga diberikan kewajiban untuk melindungi pengguna dan masyarakat luas dari kerugian yang ditimbulkan oleh Sistem Elektronik yang diselenggarakannya.

Penyelenggara sistem elektronik terutamanya dalam bidang e-commerce memiliki kewajiban untuk menjaga kerahasiaan data pengguna layanan yang ia kelola. Hal tersebut dituangkan dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Pelaksanaan Transaksi Elektronik, bahwa Penyelenggara sistem elektronik memiliki kewajiban untuk :

- (1) menjaga rahasia, keutuhan, dan ketersediaan data pribadi yang dikelolanya;
- (2) menjamin bahwa perolehan, penggunaan, dan pemanfaatan Data Pribadi berdasarkan persetujuan pemilik data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
- (3) menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik data pribadi tersebut dan

sesuai dengan tujuan yang disampaikan kepada pemilik data pribadi pada saat perolehan data.

Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Pentingnya menjamin bahwa data pribadi di Indonesia dikelola dengan sistem keamanan yang baik agar dapat meminimalisir timbulnya kejahatan pencurian atau pemboboloh informasi serta kejahatan jual beli informasi online yang mengakibatkan kerugian atas penyalahgunaan data dan informasi seseorang oleh pihak yang tidak bertanggungjawab.⁶

Berdasarkan uraian-uraian sebagaimana disebutkan diatas bahwa adanya kewajiban dari Penyelenggara Transaksi Elektronik dalam menjalankan sistemnya wajib melakukan segala upaya untuk menjamin kerahasiaan data pribadi pengguna layanan dapat terjaga. Perlindungan tersebut dimulai sejak yang bersangkutan memperoleh data pribadi tersebut hingga data pribadi tersebut dimusnahkan karena sudah tidak dipakai lagi. Adapun bentuk nyata dari perlindungan data pribadi yang dilakukan oleh Penyelenggara sistem elektronik untuk menjaga kerahasiaan data dengan berpedoman pada prinsip kehati-hatian yakni bahwa penyelenggara sistem elektronik wajib melakukan segala upaya dengan sebaik-baiknya guna mencegah agar tidak adanya kerugian yang diderita oleh para pihak baik itu penyelenggara sistem elektronik sendiri maupun pengguna layanan sistem elektronik.

Selain penyelenggara sistem elektronik yang wajib menerapkan prinsip kehati-hatian, pengguna sistem elektronik juga wajib melaksanakan prinsip tersebut dalam kegiatan transaksi elektronik yang

⁶ Aswandi, R dkk. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*. Volume 3 Nomor 2. Juni 2020. h.170.

dilakukannya. Berdasarkan ketentuan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik mengatur bahwa, “Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan”; maka hal ini membawa implikasi bahwa sepanjang tidak adanya campur tangan pihak ketiga yang tidak bertanggungjawab maka dalam pemberian data pribadi, sepenuhnya didasarkan atas persetujuan si pemilik data pribadi kepada penyelenggara sistem elektronik. Hal ini dapat menjadi upaya untuk menjamin bahwa data pribadi yang diperoleh oleh sistem elektronik didapat dari mekanisme yang halal dan sesuai dengan ketentuan peraturan perundang-undangan. Maka dari itu selain adanya upaya dari penyelenggara sistem elektronik untuk menjaga agar kerahasiaan data pribadi pengguna layanannya tetap terjaga, pemilik data pribadi juga wajib berkontribusi dalam melaksanakan prinsip kehati-hatian untuk melindungi data pribadinya.

Adapun yang dapat dilakukan oleh seorang pengguna layanan untuk memberikan perlindungan terhadap data pribadinya yakni dengan cara-cara sebagai berikut:

- a. memastikan data pribadi pengguna layanan diberikan kepada pihak yang tepat.
- b. Setiap kali melakukan transaksi secara elektronik wajib melakukan pengecekan secara teliti dan berkali-kali
- c. Memeriksa dan memastikan perizinan akses aplikasi untuk mencegah aplikasi tersebut mengakses data yang ada di perangkat milik pengguna layanan.

- d. Membaca dengan baik dan cermat syarat dan ketentuan aplikasi yang digunakan.⁷

Alasan pentingnya tindakan pengguna layanan sistem informasi elektronik untuk melakukan langkah-langkah pengamanan dalam kegiatan transaksi elektronik karena ada beberapa hal yang dapat menjadi faktor pendorong meningkatnya tindakan cybercrime seperti rendahnya kesadaran hukum masyarakat dalam merespon aktivitas cybercrime;⁸

Perlindungan data pribadi yang dilakukan oleh penyelenggara sistem elektronik dalam perlindungan data pribadi ialah dalam Permenkominfo mengenai Perlindungan Data Pribadi dalam Sistem Elektronik dalam hal pelaksanaan prinsip kehati-hatian dalam perlindungan data pribadi tersebut yakni antara lain:

- a. Penyelenggara sistem elektronik harus mempunyai aturan internal perlindungan data pribadi dan untuk upaya mencegah menghindari kegagalan perlindungan data pribadi yang dikelolanya.
- b. Penyelenggara wajib melakukan pencegahan terhadapnya kegagalan dalam perlindungan data pribadi, paling sedikit berupa kegiatan : meningkatkan kesadaran SDM untuk memberikan perlindungan data pribadi dalam sistem elektronik yang dikelolanya dan mengadakan pelatihan pencegahan perlindungan data pribadi.
- c. Menjaga kebenaran, keabsahan, kerahasiaan, kakurata, dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalsisan, penyimpanan,

⁷ Putri Zaskia Salsabila. (2019). 4 Cara Menjaga Keamanan Data Pribadi dari Kejahatan Siber, available from : <https://tekno.kompas.com/read/2019/12/11/09430057/4-cara-menjaga-keamanan-data-pribadi-dari-kejahatan-siber?page=all>. diakses tanggal 10-11-2020.

⁸ Mansur, D.MA. *loc.cit*.

penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi.

- d. Menyediakan narahubung yang mudah dihubungi oleh pemilik data pribadi terkait pengelolaan data pribadinya.⁹

B. Akibat hukum terhadap Penyelenggara Sistem Elektronik yang tidak menerapkan Prinsip Kehati-hatian dalam Penyelenggaraan Sistem Elektronik

Perlindungan data pribadi dalam sistem elektronik merupakan salah satu aspek yang wajib untuk mendapat perhatian serius dalam rangka keamanan data pribadi penggunanya. Selain asas kehati-hatian yang harus diperhatikan terdapat beberapa asas lain yang mendasari perlindungan data pribadi dalam sistem elektronik yaitu:

- a. Asas perlindungan ; artinya pemerintah wajib memberikan perlindungan data pribadi warga negaranya baik di dalam maupun di luar negeri.
- b. Asas kepentingan umum; artinya bahwa undang-undang disusun untuk melindungi kepentingan masyarakat secara luas.
- c. Asas keseimbangan; keseimbangan antara hak privasi dengan hak negara yang sah berdasarkan kepentingan umum.
- d. Asas pertanggungjawaban; artinya penyelenggaraan data pribadi harus dipertanggungjawabkan oleh penyelenggara data pribadi.

Penyelenggaraan data pribadi juga memegang prinsip keamanan data pribadi dimana, pihak penyelenggara data pribadi wajib melakukan perlindungan keamanan data pribadi dari kehilangan, penyalahgunaan, akses, pengungkapan yang tidak sah, pengubahan , atau perusakan data pribadi. Hal inilah yang membawa implikasi bahwa penyelenggara data pribadi harus melakukan segala upaya atas dasar asas atau prinsip kehati-

⁹ Karo-Karo R.P.P. (2020). *Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermartabat*. Bandung : Nusamedia. h.110.

hatian agar data pribadi yang dikelola oleh penyelenggara tersebut tidak sampai mengalami kebocoran dan disalahgunakan oleh pihak lain¹⁰. Apabila pihak penyelenggara tersebut gagal melaksanakan kewajibannya untuk menjaga keamanan dari data pribadi yang ia kelola sehingga mengakibatkan kebocoran data pribadi pengguna layanan tersebut kepada pihak lain maka ia memiliki kewajiban untuk bertanggungjawab.

Sebagaimana diatur dalam ketentuan Pasal 26 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik disebutkan bahwa setiap orang yang dilanggar haknya sebagaimana diatur dalam ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini. Atas dasar kerugian yang diderita karena kebocoran data tersebut maka gugatan diajukan ke pengadilan negeri dan diselesaikan dengan mekanisme pertanggungjawaban secara perdata.

Adapun sanksi yang akan dijatuhkan akibat adanya gugatan oleh pihak yang mengalami kerugian oleh penyelenggara sistem elektronik adalah berupa ganti kerugian yang wajib dibayarkan oleh penyelenggara sistem elektronik kepada pihak yang dirugikan. Alasan yang menjadi dasar gugatan tersebut adalah perbuatan melawan hukum yang dilakukan oleh penyelenggara sistem elektronik yang bertanggungjawab atas data pribadi yang dikelolanya didasarkan atas Pasal 1365 KUHPperdata. Sebagaimana telah disampaikan pada pembahasan diatas bahwa setiap penyelenggara sistem elektronik wajib melakukan segala tindakan untuk memastikan keamanan sistem elektroniknya sehingga data pribadi yang dikelola tidak sampai bocor kepada pihak ketiga atau disalahgunakan. Untuk itulah apabila ia tidak melakukan segala upaya berdasarkan prinsip kehati-hatian sehingga sampai ada kebocoran terhadap data pribadi dari sistem elektronik tersebut maka ia wajib

¹⁰ *Ibid.* h. 81-82

melakukan pertanggungjawaban apabila pihak yang mengalami kerugian melakukan gugatan.

Meskipun ada ketentuan hukum pidana untuk menjerat pelaku yang secara tanpa hak atau melawan hukum mengakses sistem elektronik, namun ketentuan tersebut hanya dapat menjerat pelaku yang secara aktif melakukan tindakan tersebut sebagaimana diatur dalam Pasal 30 jo Pasal 46 Undang-Undang Informasi dan Transaksi Elektronik. Tidak ada ketentuan dalam Undang-Undang ITE yang menjerat kelalaian dari Penyelenggara Sistem Elektronik yang melakukan kelalaian sehingga sampai terbukanya akses data pribadi pengguna layanan kepada pihak ketiga. Ini merupakan hal yang harus dicermati dengan seksama dalam Rancangan Undang-Undang Perlindungan Data Pribadi yang saat ini masih dibahas di parlemen, untuk menjaga agar Penyelenggara Sistem Elektronik memperketat keamanan sistemnya untuk mencegah adanya kebocoran data. Terlebih lagi dalam Rancangan Undang-Undang tentang Perlindungan Data Pribadi hanya mengatur ketentuan Pidana sebanyak 2 (dua) Pasal yang mana berkaitan dengan pencurian data pribadi.

4. Kesimpulan

Berdasarkan uraian-uraian tersebut diatas dalam tulisan ini dapat ditarik kesimpulan bahwa:

- a. Prinsip kehati-hatian dalam penyelenggaraan sistem elektronik dalam rangka perlindungan data pribadi dilaksanakan dengan adanya upaya aktif dari penyelenggara sistem elektronik selaku pihak yang mengelola data pribadi pengguna layanan untuk menjamin kerahasiaan data dan keamanan sistem elektroniknya dengan segala upaya untuk mencegah agar sistem tersebut tidak sampai dibobol oleh pihak ketiga.

- b. Akibat hukum bilamana terjadi kebocoran data pribadi maka pihak penyelenggara sistem elektronik wajib bertanggung jawab secara keperdataan dengan membayar ganti kerugian atas dasar gugatan oleh pemilik data pribadi yang mengalami kebocoran data dan/atau kerugian secara materiil maupun immateriil.

Daftar Pustaka

1. Buku

Fajar, M & Ahmad Y. (2010). *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta. Pustaka Pelajar.

Karo-Karo R.P.P. (2020). *Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermartabat*. Bandung : Nusamedia

Mansur, D. M.A. & Gultom, E. (2009). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung Refika Aditama.

2. Jurnal Ilmiah

Aswandi, R dkk. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*. Volume 3 Nomor 2. Juni 2020.

Rosadi, S.D., (2018), Perlindungan Privasi Data Pribadi dalam Era Ekonomi Digital di Indonesia, *VeJ*, Volume 4, Nomor 1.

Sautunnida, L, (2018), Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia, *Kanun Jurnal Ilmu Hukum*, Vol.20 No.2 Agustus 2018

Yuniarti, S, (2019) Perlindungan Hukum Data Pribadi di Indonesia, *Jurnal BECOS*, Vol.1 No.1 September 2019.

3. Artikel Internet

Putri Zaskia Salsabila, (2019), 4Cara Menjaga Keamanan Data Pribadi dari Kejahatan Siber,

availablefrom:<https://tekno.kompas.com/read/2019/12/11/09430057/4-cara-menjaga-keamanan-data-pribadi-dari-kejahatan-siber?page=all>, diakses tanggal 10-11-2020.

4. Peraturan Perundang-Undangan

Undang-Undang No 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia No 58 Tahun 2008m Tambahan Lembaran Negara Republik Indonesia Nomor 4843 Jo Lembaran Negara Republik Indonesia No 251 Tahun 2016 , Tambahan Lembaran Negara Republik Indonesia Nomor 5952)

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

Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. (Berita Negara Republik Indonesia No. 1829 Tahun 2016).