



Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia

M Rafifnafiah Hertianto¹

¹Fakultas Hukum Universitas Gadjah Mada, E-mail: mrafifnafiah@gmail.com

Info Artikel

Masuk : 8 Agustus 2020

Diterima : 20 April 2021

Terbit : 28 April 2021

Keywords :

Personal Data Protection; Data Breach; Law Enforcement.

Kata kunci:

Perlindungan Data Pribadi;

Pelanggaran Data Pribadi;

Penegakan Hukum.

Corresponding Author:

M Rafifnafiah Hertianto, E-mail:

mrafifnafiah@gmail.com

DOI :

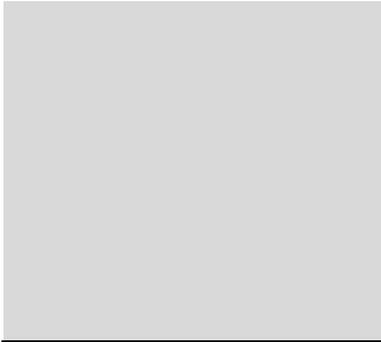
10.24843/KP.2021.v43.i01.p07

Abstract

Indonesia personal data protection law at the current moment have no specific data protection law, yet make illegal and/or unlawful action against the personal data threat increase along with the rapid technology development and information technology penetrate in Indonesia. This condition becomes an obstacle for enforcement efforts against personal data breach by certain parties that make some group of civil society as victims who can't get justice from the accident that cost them. This research aims to analyze law enforcement against personal data breach within the personal data law in Indonesia. This research uses normative juridical methods using statute approach and comparative approach and secondary data which is then analyzed to state a conclusion. Based on the analysis which has been done thus it can be concluded that the law enforcement system against personal data breach in Indonesia still not effective, even Indonesia already have some law that regulate the same subject, which caused by the absence of regulations, the anonymity of breach offender, the quality of law enforcement officer, the late response of the data manager, and the absence of specific agency that focused on the protection of personal data.

Abstrak

Belum adanya regulasi di Indonesia yang mengatur secara khusus mengenai perlindungan data pribadi membuat ancaman adanya tindakan tidak sah dan/atau melawan hukum terhadap data pribadi semakin meningkat seiring dengan tingginya laju perkembangan teknologi dan penetrasi teknologi informasi. Situasi ini tentu menjadi hambatan bagi upaya penegakan hukum terhadap kegagalan perlindungan data pribadi oleh pihak-pihak tertentu yang seringkali menempatkan sekelompok masyarakat ataupun warga negara sebagai korban yang tidak dapat mengakses keadilan terhadap peristiwa yang merugikan data pribadi mereka. Penelitian ini bertujuan untuk menganalisis bentuk penegakan hukum pelanggaran data pribadi dalam ruang lingkup hukum perlindungan data pribadi di Indonesia. Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan perundang-undangan serta perbandingan dan menggunakan data sekunder yang kemudian dilakukan analisis untuk merumuskan kesimpulan. Berdasarkan penelitian yang



telah dilakukan maka dapat disimpulkan bahwa sistem penegakan hukum terhadap kegagalan perlindungan data pribadi di Indonesia masih belum berjalan efektif meskipun Indonesia telah memiliki beberapa peraturan perundang-undangan yang mengatur hal serupa yang disebabkan oleh faktor belum adanya pengaturan yang jelas, pelaku penyerangan yang anonim, terlambatnya respons pengelola data pribadi, kualitas aparat penegak hukum, dan tidak adanya lembaga yang berfokus pada perlindungan data pribadi

1. Pendahuluan

Setiap orang sejak lahir memiliki identitas yang melekat pada dirinya berupa informasi dasar atau data yang bersifat personal atau perseorangan seperti nama, jenis kelamin, agama atau kepercayaan, golongan darah, tempat kelahiran, tanggal kelahiran, dan informasi lainnya yang akan semakin bertambah seiring bertambahnya usia orang tersebut. Umumnya data perseorangan tersebut tertera pada kartu tanda penduduk (KTP) yang dikeluarkan oleh pejabat yang berwenang ketika seseorang memasuki usia minimal yang telah ditentukan oleh peraturan perundang-undangan, kartu keluarga (KK), surat izin mengemudi (SIM), dan surat maupun kartu tanda pengenal lainnya yang dikeluarkan oleh pejabat yang berwenang. Data perseorangan yang ada pada surat dan kartu tanda pengenal yang dikeluarkan oleh pejabat yang berwenang merupakan data pribadi yang bersifat personal dan rahasia. Hal tersebut bersesuaian dengan pengertian data pribadi menurut Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan yang menyatakan bahwa data pribadi merupakan data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Perkembangan zaman dan teknologi yang semakin modern mengubah pola tingkah laku dan cara kerja manusia yang semula konvensional kemudian mengalami digitalisasi dengan berkembangnya teknologi dan internet. Hal tersebut didukung oleh survei yang dilakukan oleh Asosiasi Penyedia Jasa Internet Indonesia bahwa pengguna internet di Indonesia pada tahun 2018 mencapai 171,18 juta jiwa yang memiliki arti bahwa 64,8% dari total penduduk yang mencapai 264,16 juta jiwa pada saat itu telah aktif menggunakan internet.¹ Dalam perkembangannya, aspek-aspek kehidupan masyarakat menjadi semakin terintegrasi dengan teknologi dan internet seperti kegiatan perekonomian yang bergeser seiring maraknya *e-commerce*, sektor keuangan melalui *e-payment*, sektor formal pemerintahan yang memanfaatkan *e-government*, pelayanan administratif pengadilan yang memanfaatkan layanan *e-court* dan adanya perkembangan *cloud*

¹ Asosiasi Penyedia Jasa Internet Indonesia. Penetrasi & Profil Perilaku Pengguna Internet Indonesia 2018 Survei. Available from <https://Apjii.or.id/Content/Read/39/410/Hasil-Survei-Penetrasi-Dan-Perilaku-Pengguna-Internet-Indonesia-2018> (diakses 20 Januari 2020)

computing (komputasi awan) yaitu aplikasi yang menyediakan ruang penyimpanan data pengguna seperti *Google Drive, iCloud, Dropbox, Youtube* dan sebagainya.² Pemanfaatan layanan internet oleh masyarakat tersebut tidak terlepas dari pengiriman data pribadi seperti nama, alamat surat elektronik, kata sandi, dan data lain dari pengguna layanan yaitu masyarakat kepada penyedia layanan sebagai syarat untuk dapat memanfaatkan layanan yang disediakan tersebut. Seiring maraknya penggunaan data pribadi dalam layanan yang disediakan oleh pihak swasta maupun pemerintahan, terdapat peluang yang semakin besar bagi terjadinya pelanggaran data pribadi, terlebih lagi pada status *quo* Indonesia masih belum memiliki regulasi komprehensif mengenai perlindungan data pribadi.

Suatu pelayanan publik yang bersifat konvensional maupun digital membutuhkan data pribadi tertentu untuk dapat memproses suatu informasi atau memberikan layanan tertentu, yang mana hal tersebut memberikan beban tanggung jawab kepada penyelenggara layanan untuk mengolah, menyimpan, dan melindungi data pribadi pengguna layanan dengan baik dan hati-hati. Kedudukan data pribadi menjadi sangat penting karena data pribadi merupakan sekumpulan informasi tertentu mengenai seseorang yang mana hal tersebut memiliki nilai ekonomi tersendiri sehingga akan sangat rawan apabila disalahgunakan untuk kepentingan yang tidak selaras dengan tujuan penggunaan data pribadi.³ Kondisi tersebut menempatkan data pribadi milik seluruh rakyat Indonesia berada dalam posisi yang berbahaya akibat adanya ancaman yang besar terhadap kebocoran atau penyalahgunaan.

Perlindungan data pribadi sesungguhnya merupakan bagian daripada perlindungan konstitusional. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya, UUD NRI 1945) Pasal 28G ayat (1) yang berbunyi: "*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*" Pasal tersebut telah memberikan amanat pada penyelenggara negara untuk melaksanakan jaminan perlindungan atas privasi termasuk perlindungan terhadap data pribadi pada setiap orang. Jaminan konstitusional tersebut belum terejawantahkan dengan baik pada tingkat peraturan perundang-undangan pelaksana, meskipun setidaknya telah ada beberapa undang-undang di Indonesia dengan memiliki materi muatan yang bersinggungan atau berketerkaitan dengan perlindungan data pribadi warga negara.⁴

² Sinta Dewi. (2015). Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia. *Jurnal De Jure*, 15(2), p. 165.

³ Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). Legal Protection For Urban Online Transportation User's Personal Data Disclosure In The Age Of Digital Technology, *Padjadjaran Journal Of Law*, 5(3), 485-505, DOI: <https://doi.org/10.22304/pjih.v5n3.a5>, p. 487-488.

⁴ Lembaga Studi dan Advokasi Masyarakat. Perlindungan Data Pribadi Di Indonesia Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia. Available from

Ketika suatu data pribadi mengalami kebocoran, pencurian, atau akses yang tidak sah dan/atau melawan hukum maka dapat dikatakan bahwa pengendali data pribadi tersebut telah gagal untuk melakukan perlindungan terhadap data pribadi yang dikendalikan. Kegagalan perlindungan data sendiri belum memiliki definisi dan ruang lingkup tersendiri dalam hukum positif di Indonesia, akan tetapi jika mengacu pada *General Data Protection Regulation* maka kegagalan perlindungan data pribadi (*data breaches*) dapat diartikan sebagai pelanggaran terhadap sistem keamanan yang mengakibatkan kerusakan, kehilangan, pengungkapan dan akses secara melawan hukum dan/atau tidak sah terhadap data pribadi yang dikirim, disimpan, atau diproses yang meliputi:

1. Akses yang dilakukan oleh pihak yang tidak berwenang;
2. Tindakan secara sengaja maupun tidak sengaja yang dilakukan oleh pengontrol dan pemroses data;
3. Mengirimkan data pribadi pada penerima yang tidak berhak;
4. Perangkat komputasi yang berisi data pribadi hilang atau dicuri;
5. Perubahan data pribadi tanpa izin; dan
6. Tidak tersedianya data pribadi.

Banyak kasus yang terjadi di Indonesia menunjukkan kegagalan perlindungan data pribadi oleh pengendali data pribadi dari pihak swasta maupun pemerintahan yang umumnya berupa pencurian data, seperti peristiwa pencurian dan penyalahgunaan data yang dilakukan oleh Cambridge Analytica melalui Facebook pada bulan Maret 2018 lalu yang membuat sekitar satu juta data pengguna Facebook Indonesia turut menjadi korban.⁵ Kejadian tersebut menjadi peringatan bagi pemerintah, warga negara, dan pemangku kebijakan terkait bahwa persoalan perlindungan data pribadi menjadi sangat krusial dan perlu diselesaikan. Rancangan undang-undang perlindungan data pribadi yang diharapkan menjadi payung hukum tidak kunjung disahkan menjadikan kejadian kegagalan data pribadi seolah-olah tidak dapat ditindaklanjuti dan data pribadi warga negara terpapar ancaman.⁶ Meskipun pada Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya UU ITE) dimungkinkan untuk melakukan upaya hukum berupa pengajuan gugatan keperdataan terhadap Cambridge Analytica dan Facebook selaku pengendali dan pemroses data pribadi yang gagal melakukan perlindungan, akan tetapi pada praktiknya proses peradilan belum menemukan

<https://elsam.or.id/perindungan-data-pribadi-di-indonesia-usulan-pelembagaan-kebijakan-dari-perspektif-hak-asasi-manusia> (Diakses 20 Juli 2020).

⁵ CNN Indonesia. Kronologi Pembobolan Facebook oleh Cambridge Analytica. Available from <https://www.cnnindonesia.com/teknologi/20180322194919-185-285163/kronologi-pembobolan-facebook-oleh-cambridge-analytica> (Diakses 2 Februari 2021).

⁶ Katadata. Cambridge Analytica Dan Peran Negara Dalam Perlindungan Data Pribadi. Available from <https://katadata.co.id/Pingitfajrin/Digital/5e9a498e8de68/Cambridge-Analytica-Dan-Peran-Negara-Dalam-Perlindungan-Data-Pribadi> (Diakses 27 Juli 2020).

titik terang hingga saat ini sehingga upaya penegakan hukum terhadap hal tersebut menjadi tidak efektif dan tidak berpihak pada korban.

Saat ini Indonesia sedang mempersiapkan rancangan undang-undang perlindungan data pribadi untuk memberikan perlindungan secara optimal terhadap data pribadi sesuai amanat UUD NRI 1945.⁷ Upaya tersebut dilakukan karena mengingat kondisi ketiadaan hukum perlindungan data pribadi yang jelas dan terunifikasi maka hanya akan terdapat dua jenis pengendali data di Indonesia yaitu pengendali data yang telah mengalami kegagalan perlindungan data pribadi dan pengendali data yang akan mengalami kegagalan perlindungan data pribadi.⁸ Pengaturan data pribadi beserta penegakannya telah dimiliki Indonesia meskipun bersifat parsial dan sektoral akan tetapi masih banyak terjadi peristiwa kegagalan perlindungan data pribadi.

Berlatar belakang dari deskripsi tersebut, penelitian ini bertujuan untuk meneliti bentuk penegakan hukum terhadap kegagalan perlindungan data pribadi di Indonesia. Kajian ini menjadi sangat penting dan relevan dilakukan mengingat perkembangan zaman yang semakin meningkatnya kasus kegagalan perlindungan data pribadi yang terjadi di Indonesia yang menempatkan warga negara sebagai pemilik data dalam posisi rentan sehingga dibutuhkan suatu bentuk penegakan hukum yang jelas dan tegas untuk menjamin keamanan data pribadi. Oleh karena itu dapat ditarik rumusan masalah sebagai berikut:

1. Bagaimana konsep perlindungan data pribadi sebagai bagian dari perlindungan hak asasi manusia?
2. Bagaimana status dan bentuk penegakan hukum di Indonesia terhadap kegagalan perlindungan data pribadi?

2. Metode Penelitian

Berdasarkan jenisnya penelitian ini merupakan penelitian yuridis normatif yang memiliki arti bahwa penelitian ini dilakukan dengan memperhatikan hukum positif serta nilai dan norma hukum yang ada di masyarakat. Penelitian ini menggunakan data yang berasal dari berbagai norma hukum yang terdapat dalam perjanjian internasional, peraturan perundang-undangan dan norma-norma hukum yang ada di dalam masyarakat.⁹ Penelitian ini menggunakan beberapa pendekatan yaitu pendekatan perundang-undangan (*statute approach*) dan pendekatan perbandingan (*comparative approach*). Sumber data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri atas bahan hukum primer, sekunder, dan tersier yang didapatkan melalui studi literatur. Penelitian ini menganalisis peraturan perundang-undangan yang terkait dengan perlindungan data pribadi yang terdapat di Indonesia dengan menggunakan metode analisis

⁷ Sinta Dewi Rosadi dan Garry Gumelar Pratama. (2018). Urgensi Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia. *Jurnal Veritas Et Justitia* 4(1), 88-110, <https://doi.org/10.25123/vej.v4i1.2916>, p. 92.

⁸ Daniel J Marcus. (2018). The Data Breach Dilemma: Proactive Solutions For Protecting Consumers. *Duke Law Journal* 68. p. 558.

⁹ Zainuddin Ali. (2009). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.p. 105.

data kualitatif yang bertujuan untuk mengetahui dan memahami sistem penegakan hukum dalam ruang lingkup perlindungan data pribadi di Indonesia

3. Hasil Dan Pembahasan

3.1. Perlindungan Data Pribadi sebagai Hak Asasi Manusia

Indonesia pada saat ini belum memiliki peraturan perundang-undangan positif yang secara spesifik mengatur mengenai perlindungan data pribadi. Pengaturan data pribadi justru secara parsial tersebar di sejumlah pertauran perundang-undangan yang menjadikan definisi dan ruang lingkup data pribadi tidak seragam, sebagaimana dijelaskan pada Tabel 1. Ketidaksamaan definisi dan ruang lingkup tersebut menjadi kontraproduktif ketika dalam suatu kasus tertentu apabila hendak merujuk pada istilah data pribadi maka akan terjadi ketidakseragaman pemahaman dan konsep hukum.

Tabel 1. Definisi Data Pribadi menurut Ketentuan Peraturan Perundang-Undangan

No.	Peraturan Perundang-undangan	Perundang-undangan	Definisi
1.	Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.	24	Data pribadi adalah data perseorangan tertentu yang disimpan dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. ¹⁰
2.	Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.	71	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. ¹¹
3.	Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.	20	Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. ¹²

¹⁰ Pasal 1 angka 22 Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

¹¹ Pasal 1 angka 29 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.

¹² Pasal 1 angka 1 Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

4.	Rancangan Undang-Undang Perlindungan Data Pribadi	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. ¹³
----	---	--

Meskipun terdapat perbedaan definisi dan ruang lingkup data pribadi dalam peraturan perundang-undangan *a quo* seperti yang terdapat dalam tabel 1 hal tersebutlah tidak mereduksi makna esensial dari data pribadi itu sendiri yaitu setiap data yang bersifat perseorangan yang wajib disimpan, dirawat, dan dilindungi kerahasiaannya. Konsep data pribadi sendiri sangat lekat dengan hak asasi manusia (HAM) karena dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak atas privasi (*rights to privacy*) yang merupakan hak fundamental pada manusia.¹⁴ Pengertian dari hak pribadi sendiri yaitu hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai, dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.¹⁵ Ruang lingkup dari hak atas privasi sendiri meliputi gangguan terhadap tindakan seseorang mengasingkan diri atau menyendiri, atau gangguan terhadap relasi pribadinya, pengungkapan fakta-fakta pribadi yang memalukan secara publik, publisitas yang menempatkan seseorang secara keliru di hadapan publik, dan penguasaan tanpa ijin atas kemiripan seseorang untuk keuntungan orang lain. Penyebutan hak atas privasi (*rights to privacy*) dan hak pribadi (*privacy rights*) yang ada pada Penjelasan Pasal 26 ayat (1) UU ITE terkesan berbeda, akan tetapi keduanya memiliki poin yang sama apabila ditinjau berdasarkan definisi di ketentuan pasal tersebut telah menyatakan bahwa yang dimaksud dengan hak pribadi adalah hak untuk menikmati kehidupan pribadi bebas dari segala macam gangguan yang juga merupakan konsep dari hak atas privasi.¹⁶ Hak atas privasi apabila ditelaah lebih lanjut maka tidak mengatur sebatas hak atas informasi atau komunikasi saja, akan tetapi meliputi hal-hal sebagai berikut:

¹³ Dewan Perwakilan Rakyat. RUU Perlindungan Data Pribadi. Available from <https://www.dpr.go.id/uu/detail/id/353> (Diakses 2 Februari 2021).

¹⁴ David Banisar dan Simon Davies. (1999). Privacy & Human Rights-An International Survey Of Privacy Laws And Developments. *Journal of Computer & Information Law* 18. p.3.

¹⁵ Penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

¹⁶ Anjas Putra Pramudito. (2020). Kedudukan Dan Perlindungan Hak Atas Privasi Di Indonesia. *Jurist-diction* 3(4), 1397-1414, <http://dx.doi.org/10.20473/jd.v3i4.20212>, p. 1405.

1. Privasi informasi, yang melibatkan pembentukan peraturan yang mengatur pengumpulan dan penanganan data pribadi seperti informasi keuangan dan catatan medis.
2. Privasi tubuh, yang menyangkut perlindungan diri fisik orang terhadap prosedur invasive seperti pengujian obat dan pencarian rongga.
3. Privasi komunikasi, yang meliputi keamanan dan privasi surat, telepon, email dan bentuk komunikasi lainnya.
4. Privasi teritorial, yang menyangkut pengaturan batas intrusi ke dalam lingkungan.

Menyadari pentingnya hak atas privasi tersebut maka dibuatlah peraturan yang melindungi hak atas privasi pada tingkat internasional dan nasional. Pada tataran internasional hak atas privasi ini diatur di Deklarasi Universal Hak Asasi Manusia pada Pasal 12 yang menyatakan bahwa tidak seorangpun mendapatkan gangguan terhadap privasi, keluarga, tempat tinggal, atau serangan terhadap kehormatan dan reputasinya dan juga melindungi hak setiap orang dari suatu gangguan atau serangan. Pengaturan lebih mengikat dituangkan dalam Kovenan Internasional Hak Sipil dan Politik (Kovenan Sipol) yang diatur dalam Pasal 17 yang menyatakan hal yang sama dengan Pasal 12 Deklarasi Universal Hak Asasi Manusia. Indonesia mengakomodasi hak atas privasi meskipun tidak tertulis secara *letterlijk* pada konstitusi, akan tetapi hak atas privasi tersebut tercakup di dalam Pasal 28G ayat (1) UUD NRI 1945 yang kemudian dimanifestasikan pada UU ITE.

3.2. Analisis Hukum Positif dan *Status Quo* Indonesia terkait Penegakan Kegagalan Perlindungan Data Pribadi

Peristiwa kegagalan perlindungan data pribadi (*data breach*) sebenarnya bukanlah hal yang baru. Kondisi perkembangan teknologi informasi dan komunikasi yang cepat maka akan semakin tinggi pula rasio terjadinya upaya tindakan tidak sah dan/atau melawan hukum yang menimbulkan kegagalan perlindungan data pribadi. Di semester pertama tahun 2020 telah terjadi beberapa peristiwa kegagalan perlindungan data pribadi yang melibatkan pengendali data pribadi swasta dan pemerintahan, yaitu sebagai berikut:

1. Kegagalan data pribadi pada sektor swasta yang kebanyakan menasar pada sektor *e-commerce* seperti pada 17 April 2020. Tokopedia diduga mengalami kebocoran data pribadi penggunanya sebanyak 12.115.583 akun. Tidak lama setelah insiden itu, kembali terjadi kebocoran data yang dialami oleh Bhineka.com. Sekelompok peretas ShinyHunters mengaku memiliki 1,2 juta data pengguna. Data tersebut dihargai senilai USD 12.000 atau setara dengan Rp 17.800.000,-. Beberapa waktu sebelumnya, insiden kegagalan perlindungan data pribadi dialami oleh Bukalapak sebanyak 12.957.573 akun pengguna *platform* tersebut diperjualbelikan.¹⁷

¹⁷ Investor Daily Indonesia. Ratusan Juta Data Pengguna e-Commerce Bocor, Indonesia Harus Serius Lindungi Data Pribadi. Available from <https://investor.id/it-and-telecommunication/ratusan-juta-data-pengguna-ecommerce-bocor-indonesia-harus-serius-lindungi-data-pribadi> (Diakses 2 Februari 2021).

2. Kebocoran data tidak hanya terjadi pada sektor swasta, pada 21 Mei 2020, terdapat dugaan adanya penjualan 2 juta data pemilih di situs *dark web*. Penjual juga mengaku memiliki 200 juta data pemilih, yang meliputi nama lengkap, alamat, nomor identitas, tanggal lahir, umur, kewarganegaraan, dan jenis kelamin, yang berasal dari Daftar Pemilih Tetap (DPT) milik Komisi Pemilihan Umum (KPU) dan pada 20 Mei 2020, data warga terkait Covid-19 di Indonesia diduga telah dicuri oleh peretas. Peretas tersebut menjual data pasien terinfeksi virus corona tersebut di forum *dark web* RapidForums, data-data warga yang dijual itu terbilang lengkap. Beberapa informasi tersebut, antara lain nama, status kewarganegaraan, tanggal lahir, umur, nomor telepon, alamat rumah, Nomor Identitas Kependudukan (NIK), dan hasil tes Covid-19 juga muncul secara detail dalam basis data tersebut. Data yang dijual berupa gejala, tanggal mulai sakit, dan tanggal pemeriksaan.¹⁸

Peristiwa yang telah menimpa sejumlah sektor di Indonesia tersebut semakin memperlihatkan kondisi perlindungan data pribadi Indonesia yang sangat rentan, akan tetapi penegak hukum di Indonesia hingga saat ini masih belum dapat menjalankan tugasnya secara optimal untuk melindungi korban dari peristiwa kegagalan perlindungan data pribadi. Berikut merupakan faktor yang menyebabkan kurang optimalnya penegakan hukum terhadap kegagalan perlindungan data pribadi:

1. Belum adanya ketentuan peraturan perundang-undangan mengenai model dan bentuk penegakan hukum yang jelas dan terunifikasi terhadap kegagalan perlindungan data pribadi. Sampai saat ini ketentuan yang mengatur mengenai sanksi terhadap tindakan tidak sah dan/atau melawan hukum terhadap data pribadi tersebar di beberapa peraturan perundang-undangan yang bersifat parsial dan sektoral sehingga penegakan hukum terhadapnya seringkali mengalami kebingungan untuk menggunakan ketentuan yang mana. Apabila menelaah lebih lanjut ketentuan penegakan hukum dalam peraturan perundang-undangan *a quo* pendekatan yang digunakan berorientasi kepada pemidanaan sebagai *primum remidium*, menurut beberapa akademisi hukum bahwa pemidanaan sebagai *ultimum remidium* memang diperlukan untuk memberi efek jera akan tetapi, pidana yang dijatuhkan jangan sampai terlalu memberatkan karena akan melumpuhkan industri dan dikhawatirkan pemidanaan justru menjadi alat penambah kerugian bagi korban.¹⁹

¹⁸ Lembaga Studi dan Advokasi Masyarakat. Akselerasi Pembahasan RUU Pelindungan Data Pribadi Mendesak. Available from <https://elsam.or.id/Marak-Insiden-Kebocoran-Dataakselerasi-Pembahasan-Ruu-Pelindungan-Data-Pribadi-Mendesak/> (Diakses 22 Juli 2020).

¹⁹ Balairung Press. Legislasi sebagai Solusi Kasus Pencurian Data. Available from <http://www.balairungpress.com/2020/03/legislasi-sebagai-solusi-kasus-pencurian-data/> (Diakses 24 Juli 2020).

Tabel 2. Ketentuan Sanksi terhadap Pelanggaran Data Pribadi pada Peraturan Perundang-Undangan di Indonesia.

No.	Peraturan Perundang-Undangan	Bentuk Penegakan Hukum	Ketentuan Sanksi
1.	Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.	Sanksi Pidana, Gugatan Keperdataan, dan Alternatif Penyelesaian Sengketa	<ol style="list-style-type: none"> 1) Sanksi pidana terhadap akses secara tanpa hak atau melawan hukum terhadap komputer atau sistem elektronik untuk mendapatkan informasi elektronik.²⁰ 2) Sanksi pidana terhadap perbuatan tanpa hak atau melawan hukum mengubah, merusak, menghilangkan, memindahkan, membuka, atau menyembunyikan Informasi Elektronik dan/atau Dokumen Elektronik.²¹ 3) Gugatan perdata terhadap pihak yang menimbulkan kerugian atau melanggar hak.²² 4) Mekanisme alternatif penyelesaian sengketa yang dapat dilakukan selain mengajukan gugatan perdata.²³
2.	Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang	Sanksi Pidana	Sanksi pidana terhadap pemberian keterangan tentang nasabah bank yang dirahasiakan secara melawan hukum atau tidak

²⁰ Pasal 46 jo. Pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

²¹ Pasal 48 jo. Pasal 32 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

²² Pasal 26 dan Pasal 38 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

²³ Pasal 39 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

	Nomor 7 Tahun 1992 Tentang Perbankan.		dalam keadaan yang dikecualikan undang-undang. ²⁴
3.	Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.	Sanksi Pidana	1) Sanksi pidana terhadap perbuatan tanpa hak mengubah, mengurangi, dan menambah data kependudukan. ²⁵ 2) Sanksi pidana terhadap perbuatan tanpa hak mengakses data kependudukan. ²⁶
4.	Undang Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.	Sanksi Pidana	Larangan pembukaan informasi yang mengandung informasi rahasia yang dapat menimbulkan kerugian bagi negara dan warga negara. ²⁷
5.	Rancangan Undang-Undang Perlindungan Data Pribadi. ²⁸	Sanksi Pidana dan Administratif	1) Pasal 50 mengenai sanksi administratif berupa: a. peringatan tertulis; b. penghentian sementara kegiatan pemrosesan data pribadi; c. penghapusan atau pemusnahan data pribadi; d. ganti kerugian; dan/atau e. denda administratif. 2) Bab XIII mengenai ketentuan pidana bagi setiap orang termasuk korporasi.

²⁴ Pasal 47 jo. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.

²⁵ Pasal 94 Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

²⁶ Pasal 95 Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

²⁷ Pasal 54 jo. Pasal 17 Undang Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

²⁸ Dewan Perwakilan Rakyat. RUU Perlindungan Data Pribadi. Available from <https://www.dpr.go.id/uu/detail/id/353> (Diakses 2 Februari 2021).

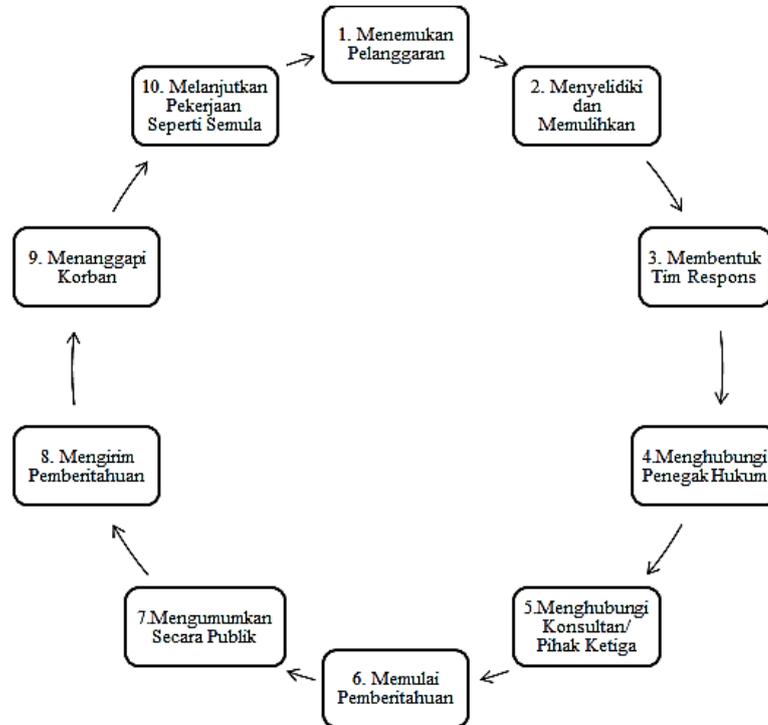
2. Identitas pelaku penyerangan terhadap data pribadi tersebut kebanyakan tidak dapat diketahui atau diidentifikasi sehingga menyulitkan penegak hukum untuk melacak aktor yang dianggap bertanggung jawab.²⁹ Peristiwa kegagalan perlindungan data pribadi sangat erat kaitannya dengan isu keamanan siber yang mana dalam ranah keamanan siber seringkali tidak diketahui secara pasti siapa aktor penyerangan sistem keamanan siber karena siapapun dapat menjadi aktor penyerang sistem keamanan siber.³⁰ Untuk mengatasi hal tersebut maka diperlukan pengendalian dan pengawasan terhadap lalu lintas jaringan internet, kendatipun dalam beberapa aspek dapat mengakibatkan terganggunya hak atas privasi. Oleh karena itu dalam pengembangan sistem keamanan perlu untuk menemukan titik tengah keseimbangan antara keamanan dan privasi agar tidak mengorbankan privasi publik.³¹
3. Berdasarkan peristiwa kegagalan perlindungan data pribadi yang telah terjadi tersebut pengendali data pribadi baru mengetahui bahwa adanya tindakan tidak sah dan/atau melawan hukum terhadap data pribadi yang dikendalikan baru setelah tindakan tersebut terjadi atau setelah berita terhadap peristiwa tersebut mencuat sehingga tidak adanya tindakan optimal yang dilakukan oleh pengendali data pribadi. Tidak sedikit pula pengendali data pribadi yang merespons bahwa tidak ada upaya tindakan secara tidak sah dan/atau melawan hukum terhadap data yang dikendalikannya, padahal secara publik pihak peretas telah menunjukkan bukti data pribadi yang berhasil diambilnya secara tidak sah dan/atau melawan hukum. Kondisi tersebut tidak memberikan pengendali data pribadi pilihan bertindak untuk menyelamatkan data pribadi atau menyelamatkan reputasi keamanan sistem perlindungan data yang dimilikinya.

²⁹ Vannyora Okditazeini dan Irwansyah. (2018). Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS). *Jurnal Studi Komunikasi Dan Media*, 22 (2). 109-122 DOI: <http://dx.doi.org/10.31445/jskm.2018.220202> p. 114.

³⁰ Hans De Bruijn dan Marijn Janssen. (2017). Building Cybersecurity Awareness: The Need For Evidence-Based Framing Strategies. *Government Information Quarterly Journals*, 34.p. 6.

³¹ Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A.. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, 32.p. 136.

Diagram 1. Alur Respons dan Tindakan yang Dilakukan Saat Terjadi Kegagalan Perlindungan Data Pribadi³²



Alur tersebut menunjukkan kewajiban bagi setiap pengendali data pribadi apabila terjadi kegagalan perlindungan data pribadi pada sistem yang dikendalikannya. Peristiwa yang kerap terjadi di Indonesia yaitu apabila pengendali data pribadi menemukan adanya tindakan secara tidak sah dan/atau melawan hukum terhadap data pribadi yang dikendalikannya, pengendali data pribadi tersebut tidak melakukan tindakan yang disyaratkan pada alur tersebut yang mana hal tersebut dapat dikatakan sebagai kelalaian pengendali data pribadi dan sistem perlindungan data pribadi yang dimilikinya.

4. Kualitas sumber daya manusia aparat penegak hukum yang belum optimal dalam menguasai dan memahami isu hukum dalam perkembangan teknologi. Salah satu faktor penentu kualitas penegakan hukum ialah bagaimana kualitas dari aparat penegak hukum dalam mengaplikasikan keahlian dan pengetahuan yang dimilikinya untuk menyelesaikan suatu isu hukum. Layaknya isu keamanan siber yang belum lama ini semakin berkembang di Indonesia, isu hukum dalam perlindungan data pribadi pun seolah menjadi fenomena baru di ranah hukum Indonesia. Kondisi di lapangan menyatakan bahwa tidak banyak

³² Charles Devoel dan Syed (Shawon) M. Rahman,. (2013). Incident Response Plan For A Small To Medium Sized Hospital. *International Journal Of Network Security & Its Applications*, 5(2). p. 4-9.

aparatus penegak hukum yang memahami seluk-beluk teknologi informasi, selain itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi isu kegagalan perlindungan data pribadi berbasis teknologi karena masih banyak aparat penegak hukum gagap teknologi yang disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet yang memadai.³³

5. Tidak adanya lembaga yang mengawasi dan menilai sistem perlindungan data pribadi serta melindungi hak korban. Eksistensi lembaga pengawas pada praktik penegakan hukum perlindungan data pribadi menjadi penting karena pada *status quo* peristiwa kegagalan perlindungan data pribadi seolah-olah hanya menjadi tanggung jawab dari pihak yang mengalami kegagalan melindungi data pribadi saja tanpa adanya peran pemerintah selaku regulator untuk melindungi negara dan warga negaranya. Meskipun Badan Siber dan Sandi Negara (BSSN) kerap ditunjuk sebagai lembaga yang berwenang untuk menangani peristiwa kegagalan perlindungan data pribadi, akan tetapi sering pula terjadi saling lempar tanggung jawab antara BSSN dan Kementerian Komunikasi dan Informasi khususnya Direktorat Jendral Aplikasi Informatika (Ditjen Aptika). Apabila melakukan perbandingan dengan praktik kelembagaan yang menangani terkait perlindungan data pribadi di Inggris yang memiliki lembaga khusus bernama *Information Commissioners Office (ICO)*. Lembaga tersebut memiliki kewenangan untuk mengawasi praktik perlindungan data pribadi, melakukan audit terhadap sistem perlindungan data pribadi, menerima laporan mengenai isu perlindungan data pribadi, menegakkan aturan yang ada pada *General Data Protection Regulation*, menjatuhkan sanksi apabila terjadi kegagalan perlindungan data pribadi, melakukan penyelidikan terhadap peristiwa kegagalan perlindungan data pribadi, sampai melakukan kerjasama internasional yang dinilai perlu untuk meningkatkan perlindungan data pribadi.³⁴ Melihat perbandingan tersebut membuat urgensi dibentuknya lembaga khusus perlindungan data pribadi semakin diperlukan. Kualitas sumber daya manusia selaku penegak hukum dalam hal perlindungan data pribadi juga turut menyumbang urgensi pembentukan lembaga khusus tersebut, pada *status quo* tidak banyak aparat penegak hukum yang memahami persoalan dan penanganan data pribadi yang membuat penegakan hukum terhadapnya semakin tidak efektif. Lembaga khusus tersebut nantinya akan melakukan penegakan hukum lebih efektif dibandingkan lembaga yang ada saat ini dikarenakan sumber daya manusia dari lembaga khusus tersebut yang memang merupakan praktisi yang memahami persoalan data pribadi.

³³ Ahmad S. Daud. (2013). Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi. *Jurnal Lex Crimen*, 3(1), p. 101.

³⁴ Ewan Nettleton dan Charles Willison. (2010). Data Protection: More Powers For The Information Commissioner. *Jurnal Of Database Marketing & Customer Strategy Management*, 17(2), p. 134.

4. Kesimpulan

Perlindungan data pribadi sebagai hak atas privasi merupakan bagian dari perlindungan hak asasi warga negara sebagaimana yang tercantum dalam konstitusi dan hukum positif negara Indonesia yang harus dilindungi dan dilakukan penegakan hukum apabila terdapat pelanggaran terhadapnya. Sistem penegakan hukum terhadap peristiwa kegagalan perlindungan data pribadi di Indonesia masih belum efektif yang dikarenakan faktor belum adanya pengaturan yang jelas, pelaku penyerangan yang anonim, terlambatnya respons pengelola data pribadi, kualitas aparat penegak hukum, dan tidak adanya lembaga yang berfokus pada perlindungan data pribadi. Penegakan hukum yang belum efektif tersebut memiliki arti bahwa negara masih belum berhasil memberikan perlindungan dan rasa aman terhadap hak atas privasi warga negara. Meskipun Indonesia telah memiliki beberapa peraturan perundang-undangan yang memiliki materi muatan berupa perlindungan data pribadi, akan tetapi hal tersebut tidak memberikan jaminan bahwa penegakan hukum terhadap kegagalan perlindungan data pribadi telah berjalan dengan baik yang mana terbukti dari beberapa peristiwa kegagalan perlindungan data pribadi yang tidak berujung dan tidak berpihak pada korban.

Daftar Pustaka / Daftar Referensi

Buku

Ali, Z. (2009). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Jurnal

Banisar, David dan Davies, S. (1999). Privacy & Human Rights-An International Survey Of Privacy Laws And Developments. *Journal Of Computer & Information Law*, 18.

Bruijn, H.D. dan Janssen, M. (2017). Building Cybersecurity Awareness: The Need For Evidence-Based Framing Strategies. *Government Information Quarterly Journals*, 34.

Daud, A.S. (2013). Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi. *Jurnal Lex Crimen*, 3(1).

Devoel, C. dan Rahman. S. M. (2013). Incident Response Plan For A Small To Medium Sized Hospital. *International Journal Of Network Security & Its Applications*, 5(2).

Dewi, S. (2015). Privasi Atas Data Pribadi: Perlindungan Hukum Dan Bentuk Pengaturan Di Indonesia. *Jurnal De Jure*, 15(2).

Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions For Protecting Consumers. *Duke Law Journal*, 68.

Nettleton, E. dan Willison, C. (2010). Data Protection: More Powers For The Information Commissioner. *Database Marketing & Customer Strategy Management* 17(2).

- Okditazeini V. dan Irwansyah. (2018). Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS). *Jurnal Studi Komunikasi Dan Media* 22 (2). 109-122 DOI: <http://dx.doi.org/10.31445/jskm.2018.220202>.
- Pramudito, A.P. (2020). Kedudukan Dan Perlindungan Hak Atas Privasi Di Indonesia. *Jurist-diction* 3(4), 1397-1414, <http://dx.doi.org/10.20473/jd.v3i4.20212>.
- Reddick, C. G., Chatfield, A. T., dan Jaramillo, P. A. (2015). Public Opinion On National Security Agency Surveillance Programs: A Multi-Method Approach. *Government Information Quarterly Journals*, 32.
- Sinta Dewi Rosadi dan Garry Gumelar Pratama. (2018). Urgensi Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia. *Jurnal Veritas Et Justitia* 4(1), 88-110, <https://doi.org/10.25123/vej.v4i1.2916>.
- Tejomurti, K., Hadi, H., Imanullah, M. N., dan Indriyani, R. (2018). Legal Protection For Urban Online Transportation User's Personal Data Disclosure In The Age Of Digital Technology. *Padjadjaran Journal Of Law*, 5(3).

Online/World Wide Web:

- Asosiasi Penyedia Jasa Internet Indonesia. (2019). Penetrasi & Profil Perilaku Pengguna Internet Indonesia 2018 Survei. Retrieved from <https://Apjii.Or.Id/Content/Read/39/410/Hasil-Survei-Penetrasi-Dan-Perilaku-Pengguna-Internet-Indonesia-2018>, diakses 20 Januari 2020.
- Balairung Press. (2020). Legislasi sebagai Solusi Kasus Pencurian Data. Retrieved from <http://www.balairungpress.com/2020/03/legislasi-sebagai-solusi-kasus-pencurian-data/>, diakses 24 Juli 2020.
- CNN Indonesia. (2018) Kronologi Pembobolan Facebook oleh Cambridge Analytica. Retrieved from <https://www.cnnindonesia.com/teknologi/20180322194919185285163/kronologi-pembobolan-facebook-oleh-cambridge-analytica>, diakses 2 Februari 2021.
- Dewan Perwakilan Rakyat. (2019). RUU Perlindungan Data Pribadi. Retrieved from <https://www.dpr.go.id/uu/detail/id/353>, diakses 2 Februari 2021.
- Investor Daily Indonesia. (2020). Ratusan Juta Data Pengguna e-Commerce Bocor, Indonesia Harus Serius Lindungi Data Pribadi. Retrieved from <https://investor.id/it-and-telecommunication/ratusan-juta-data-pengguna-ecommerce-bocor-indonesia-harus-serius-lindungi-data-pribadi>, diakses 2 Februari 2021.
- Katadata. (2020). Cambridge Analytica Dan Peran Negara Dalam Perlindungan Data Pribadi. Retrieved from <https://katadata.co.id/Pingitfajrin/Digital/5e9a498e8de68/Cambridge-Analytica-Dan-Peran-Negara-Dalam-Perlindungan-Data-Pribadi>, diakses 27 Juli 2020.
- Lembaga Studi dan Advokasi Masyarakat. (2016). Perlindungan Data Pribadi Di Indonesia Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi

Manusia. Retrieved from <https://elsam.or.id/perlindungan-data-pribadi-di-indonesia-usulan-pelembagaan-kebijakan-dari-perspektif-hak-asasi-manusia>, diakses 20 Juli 2020.

Lembaga Studi dan Advokasi Masyarakat. (2020). Marak Insiden Kebocoran Data, Akselerasi Pembahasan RUU Pelindungan Data Pribadi Mendesak. Retrieved from <https://elsam.or.id/Marak-Insiden-Kebocoran-Dataakselerasi-Pembahasan-Ruu-Pelindungan-Data-Pribadi-Mendesak/>, diakses 22 Juli 2020.

Peraturan perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790).

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran Negara Republik Indonesia Nomor 4674).

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846).

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400).

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 1829).