

BAB II

KAJIAN TEORETIK PERLINDUGAN DAN TANGGUNGJAWAB PENYEDIA LAYANAN ATAS KERAHASIAAN DATA PRIBADI

A. Tjauan Umum tentang Perlindungan Data Pribadi

1. Pengertian Perlindungan Data Pribadi

Informasi merupakan suatu media yang sangat menentukan bagi perkembangan ekonomi suatu negara baik negara berkembang maupun negara maju.³¹ Dengan munculnya era komputer sekarang ini menciptakan ancaman yang lebih besar bagi privasi individu, serta kemungkinan individu mengalami kerugian besar akibat ketidak telitian atau pembocoran informasi akan jauh lebih besar.³² Era digital telah memicu ledakan pertumbuhan data pribadi yang dibuat, disimpan dan ditsransmisikan pada komputer dan perangkat mobile, broadband dan situs internet dan media.³³ Kemajuan teknologi menjadi ancaman serius bagi privasi pribadi dan keamanan informasi.

Dalam hukum telematika, data merupakan representasi formal suatu konsep, fakta, atau instruksi. Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Data adalah bentuk jama dari datum, berasal dari bahasa Latin yang berarti “sesuatu yang

³¹Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasioanl*. Widya Padjajaran, Bandung. 2009. hlm 53.

³²Paul Marrett, *Informasi Law in Practice*. Edisi ke-2. MPG Books, Cornwall. 2002. Hlm 95.

³³Cameron G. Shilling, “Privacy and Data Security : New Challenges of The Digital Age” *New Hampshire Bar Journal*, 2011, hlm 1.

diberikan”.³⁴ Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan.³⁵

Data adalah sekumpulan fakta kasar yang masih perlu diolah agar bermakna. Sementara itu informasi adalah data yang diinterpretasikan dengan berbagai cara yang berarti, melalui prosedur dan alat bantu tertentu dengan basisnya pada pengetahuan. Data, bahan baku informasi, didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan, benda, dan sebagainya. Data terbentuk dari karakter yang dapat berupa alphabet, angka, maupun simbol khusus. Data disusun untuk diolah dalam bentuk struktur data, struktur file, dan data base.³⁶

Data pribadi adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi. Pembahasan dalam tulisan ini dibatasi pada data pribadi yang berkaitan langsung dengan data elektronik. Istilah perlindungan data pertama kali digunakan di Jerman dan Swedia pada tahun 1970an yang mengatur perlindungan data pribadi melalui undang-undang. Alasan dibuatnya perlindungan

³⁴Purwanto, “Penelitian Tentang Perlindungan Hukum Data Digital”, *Laporan Penelitian* Jakarta, Badan Pembinaan Hukum Nasional, 2007. hlm 13.

³⁵Radian Adi Nugraha, “Analisa Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik”, *Skripsi*, Jakarta, Universitas Indonesia, 2012.

³⁶Purwanto, *Op. Cit.* hlm 14.

karena pada waktu itu mulai dipergunakan komputer sebagai alat untuk menyimpan data penduduk, terutama untuk keperluan sensus penduduk. Ternyata dalam praktiknya, telah terjadi banyak pelanggaran yang dilakukan baik oleh pemerintah maupun pihak swasta. Karena itu agar penggunaan data pribadi tidak disalahgunakan maka diperlukan pengaturan.³⁷ Tiap-tiap negara menggunakan peristilahan yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantif kedua istilah tersebut mempunyai pengertian yang hampir sama sehingga kedua istilah tersebut sering digunakan bergantian.³⁸ Amerika Serikat, Kanada, dan Australian menggunakan istilah informasi pribadi sedangkan negara-negara Uni Eropa dan Indonesia sendiri dalam Undang-undang Informasi dan Transaksi Elektronik menggunakan istilah data pribadi.

Data pribadi terdiri atas fakta-fakta, komunikasi atau pendapat yang berkaitan dengan individu yang merupakan informasi sangat pribadi atau sensitive sehingga orang yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain. Data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.³⁹ Bentuk perlindungan terhadap data dibagi dalam dua kategori yaitu, bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik yang kasat mata maupun data

³⁷Shinta Dewi, *Op. Cit*, hlm 37.

³⁸Shinta Dewi, *Ibid*, hlm 71.

³⁹Jerry Kang, "Information Privacy in Cyberspace Transaction", *Stanford Law Review* Vol 50, 1998, hlm 5.

yang tidak kasat mata.⁴⁰ Bentuk perlindungan data yang lain adalah adanya regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu dan perusakan terhadap data itu sendiri.

2. Batas – batas Privasi

Dalam sejarah perkembangannya, privasi⁴¹ merupakan suatu konsep yang bersifat universal dan dikenal di berbagai negara baik dalam bentuk undang-undang maupun dalam bentuk aturan etika.⁴² Seperti contoh di Belanda dikenal dengan istilah *dignitas* yang berarti hak pribadi, di Jerman dikenal dengan *personlichkeitsrecht* yang berarti hak pribadi sebagai perwujudan kepribadian seseorang, sedangkan di Swiss dikenal istilah *Geheimssphäre* yang berarti privasi individu.⁴³

Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandeis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul “The Right to Privacy” atau hak untuk tidak diganggu.⁴⁴ Dalam jurnal tersebut menurut Warren dan

Brandeis dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa

⁴⁰Purwanto, *Op. Cit*, hlm 13.

⁴¹Terdapat konsep yang agak samar mengenai privasi dan keamanan (di dunia cyber). Privasi biasanya digunakan mengenai harapan bahwa seorang individu memiliki informasi tertentu yang tidak digunakan atau diungkapkan kepada pihak ketiga kecuali melalui persetujuan individu. Keamanan biasanya berarti tindakan yang akan diambil untuk memastikan informasi tentang seorang individu tertentu tersebut tidak diungkapkan kepada mereka yang tidak memiliki otoritas untuk mengakses informasi.

⁴²Shinta Dewi, *Op. Cit*, hlm 7.

⁴³Shinta Dewi, *Ibid*, hlm 8.

⁴⁴Shinta Dewi, *Ibid*, hlm 10.

ada hak seseorang untuk menikmati hidup. Hak untuk menikmati hidup tersebut diartikan sebagai hak seseorang untuk tidak diganggu kehidupan pribadinya baik oleh orang lain, atau oleh negara. Oleh karena itu hukum harus mengakui dan melindungi hak privasi tersebut .

Alasan privasi harus dilindungi yaitu⁴⁵: *Pertama*, dalam membina hubungan dengan orang lain, seseorang harus menutup sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. *Kedua*, seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (solitude) sehingga privasi sangat diperlukan oleh seseorang. *Ketiga*, privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hal lain akan tetapi hak ini akan hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. *Keempat*, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai “the right against the word”. *Kelima*, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai dimana kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapat kompensasi.

⁴⁵Shinta Dewi, *Ibid*, hlm 11.

Privasi merupakan suatu konsep yang sangat sulit untuk didefinisikan karena setiap orang akan memberi batasan yang berbeda tergantung dari sisi mana orang akan menilainya.⁴⁶ Menurut Kamus Besar Bahasa Indonesia, privasi berarti bebas, kebebasan atau keleluasaan. Kajian mengenai perkembangan kerahasiaan pribadi pada tataran masyarakat internasional yang juga menjunjung tinggi nilai-nilai yang memberikan jaminan dan perlindungan kehormatan atas diri pribadi, sehingga dimuat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM)/Universal Declaration of Human Rights (UDHR) Pasal 12, yang menyatakan: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.* (Tidak seorang pun akan mengalami gangguan sewenang-wenang dengan privasi, keluarga, rumah atau korespondensi, atau serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu)

Secara substantive, pengaturan privasi di dalam Pasal 12 UDHR ini sangat luas karena terdiri dari⁴⁷ :

1. *Physical Privacy* yaitu perlindungan privasi yang berkaitan dengan tempat tinggalnya.

⁴⁶Shinta Dewi, *Ibid*, hlm 14.

⁴⁷Shinta Dewi, *Ibid*. hlm 24.

2. *Decisional Privacy* yaitu perlindungan privasi terhadap hak untuk menentukan kehidupannya sendiri termasuk kehidupan keluarganya.
3. *Dignity* yaitu melindungi harga diri seseorang termasuk nama baik dan reputasi seseorang.
4. *Informational Privacy* yaitu privasi terhadap informasi artinya hak untuk menentukan cara seseorang melakukan dan menyimpan informasi pribadinya.

Selain dari pengaturan UDHR, Kovenan Internasional tentang HakHak Sipil dan Politik atau International Covenant on Civil and Political Rights (ICCPR) 1966 yaitu dalam Pasal 17:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation* (Tidak seorang pun akan mengalami gangguan sewenang-wenang atau melanggar hukum dengan privasi, keluarga, rumah atau korespondensi, atau serangan tidak sah atas kehormatan dan reputasinya)
2. *Everyone has the right to the protection of the law against such interference or attacks* (Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu)

Pengaturan privasi di dalam Pasal 17 tersebut menambah kata *arbitrary* atau *unlawful* atau secara melawan hukum sehubungan negaranegara tidak hanya diberi kewajiban untuk melindungi warga negaranya melalui pengaturan tetapi juga harus melarang pelanggaran privasi tersebut.⁴⁸

⁴⁸Shinta Dewi, *Ibid.* hlm 25.

Privasi sebagai suatu hak yang melekat pada setiap individu dapat dibagi menjadi beberapa jenis, yaitu ⁴⁹:

- a. Privasi atas Informasi Privasi atas informasi di antaranya menyangkut informasi pribadi, data diri, rekaman medis, pos elektronik, anonimitas online, enkripsi data, dan hak-hak khusus lainnya.
- b. Privasi Fisik Privasi fisik adalah bentuk privasi sebagai suatu hak untuk tidak ditekan, dicari, maupun ditangkap oleh pemerintah, yang pada umumnya berlaku bagi individu yang menggunakan kebebasan berpendapat dan berasosiasinya.
- c. Privasi untuk Menentukan Jati Diri Privasi untuk menentukan jati diri adalah kebebasan seorang individu untuk menentukan apa yang diinginkan tanpa campur tangan dari pihak lain, salah satu bentuk privasi ini adalah untuk melakukan aborsi, bunuh diri, transgender, dan hal-hal sejenisnya.
- d. Privasi atas Harta Benda Privasi atas harta benda adalah hak individual untuk memiliki identitas, kekayaan intelektual, dan kekayaan fisik.

Hak mengemukakan pendapat, berkumpul, dan berserikat, serta privasi yang melekat sebagai suatu hak yang paling mendasar bagi hak atas informasi atas seseorang, tidak dapat diganggu gugat oleh siapapun,

⁴⁹Danrivanto Budhijanto, "The Present and Future of Communication and Information Privacy in Indonesia", *Jurnal Hukum Internasional*, Vol. 2 No. 2, Universitas Padjadjaran, 2003, hlm. 140.

termasuk aparat pemerintah. Negara melalui pemerintah perlu memberikan jaminan atas perlindungan dari upaya ataupun tindakan yang bertujuan untuk melanggar hak-hak tersebut.

Informasi yang berkaitan dengan privasi terdapat dalam beragam bentuk dan tergantung kepada definisi dimana informasi tersebut diterapkan. Simson Garfinkel mengelompokkan informasi privasi ke dalam 5 kategori yaitu ⁵⁰:

1. *Personal Information*, informasi yang berkaitan dengan seseorang, diantaranya; nama, tanggal lahir, sekolah, nama orang tua, dan lain-lain.
2. *Private Information*, informasi yang berkaitan dengan seseorang namun tidak secara umum diketahui dan beberapa diantaranya dilindungi oleh hukum. Contoh: transkrip akademik, catatan perbankan, dan lain-lain.
3. *Personally Identifiable Information*, informasi yang diturunkan yang berasal dari seseorang berupa kebiasaan, hal-hal yang disukai, dan lain-lain.
4. *Anonymized Information*, informasi yang berkaitan dengan seseorang yang telah dimodifikasi sedemikian rupa sehingga informasi tersebut bukan merupakan informasi yang sebenarnya.

⁵⁰Efrizal Fikri Yumansyah, “*Proteksi Internet Privacy dengan Protokol P3P*” (<http://www.cert.or.id/~budi/courses/ec7010/2004-2005/fikri-report/report-fikri-23203089.doc>). Diakses pada 5 Februari 2019

5. *Aggregate Information*, informasi statistik yang merupakan gabungan dari beberapa informasi individu

3. Keamanan dan Kerahasiaan Data dalam Teknologi Informasi

Seiring dengan pesatnya kemajuan di teknologi informasi, data menjadi suatu komoditi yang eksklusif. Perlindungan akan data saat ini menjadi fenomena yang menarik karena itu tindakan-tindakan pencegahan atas kerusakan data dan informasi perlu mendapatkan pemikiran perlindungannya.⁵¹ Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang.

Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan, dan sistem-sistem setingkat itu membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan oleh kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, dimanapun, dan kapanpun mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan data dalam suatu jaringan komputer, diperlukan beberapa jenis enkripsi⁵² agar data tidak dapat dibaca atau dimengerti oleh

⁵¹Pengrusakan data disini adalah penghapusan atau perubahan data sehingga tidak dapat digunakan lagi ataupun penggunaan data oleh pihak-pihak yang tidak berwenang.

⁵²Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti atau tidak terbaca. Enkripsi dapat diartikan sebagai kode atau chipper. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk

sembarangan orang kecuali untuk penerima yang berhak. Pengamanan data tersebut selain bertujuan untuk meningkatkan keamanan data, juga berfungsi untuk : ⁵³

1. Melindungi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak;
2. Mencegah agar orang-orang yang tidak berhak, tidak menyisipkan atau menghapus data

Selain keamanan dan kerahasiaan data dalam jaringan komputer, konsep ini juga berlaku untuk keamanan dan kerahasiaan data pada internet. Hal ini mengingat bahwa kemajuan yang dicapai dalam bidang pengembangan sistem operasi komputer sendiri dan utilitasnya sudah sedemikian jauh dimana tingkat performansi, kehandalan dan fleksibilitas software menjadi kriteria utama dan berharganya informasi tersebut dan ditunjang oleh kemampuan pengembangan software tentunya menarik minat para pembobol (hacker) dan penyusup (intruder).

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek paling penting dari suatu sistem informasi. Hal ini terkait dengan begitu pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang tidak berhak. Oleh karena itu pengamanan dalam sistem informasi telah menjadi isu hangat ketika

kasus private key cryptography) atau dengan kunci yang berbeda (untuk kasus public key cryptography).

⁵³Purwanto. *Ibid.* hlm 56.

transaksi elektronik mulai diperkenalkan. Tanpa pengamanan yang ketat dan canggih, perkembangan teknologi informasi tidak memberikan manfaat yang maksimal kepada masyarakat.⁵⁴

Terhubungnya sebuah sistem informasi dengan Internet membuka peluang adanya kejahatan melalui jaringan komputer. Hal ini menimbulkan tantangan bagi penegak hukum. Hukum dari sebagian besar negara di dunia belum menjangkau daerah cyberspace. Saat ini hampir semua negara di dunia berlomba-lomba untuk menyiapkan landasan hukum bagi internet. Terkait dengan masalah yang terjadi dan perlunya pengamanan terhadap data yang ada dalam komputer, lingkup keamanan data dari suatu sistem komputer mencakup hal-hal yang tidak saja berkaitan dengan keamanan fisik, keamanan akses, keamanan file dan data, keamanan jaringan, tetapi terdapat hal-hal lainnya⁵⁵. Ancaman paling signifikan terhadap keamanan dari sistem komputer pada saat ini bukan berupa ancaman terhadap keamanan fisik, tetapi juga ancaman terhadap keamanan non-fisik yang dapat dibagi dalam 2 (dua) kategori yaitu⁵⁶ :

Intrudes dan Malicious Program⁵⁷

⁵⁴Radian Adi Nugraha, Op. Cit, hlm. 26.

⁵⁵Purwanto. *Ibid.* hlm 49.

⁵⁶Purwanto, *Ibid.* hlm 50.

⁵⁷Malicious Program termasuk virus komputer, worm, trojan, spyware dan program lain yang dibuat secara khusus untuk memata-matai lalu lintas jaringan, merekam komunikasi pribadi, menjalankan perintah yang tidak sah, mencuri dan mendistribusikan informasi pribadi dan rahasia, menonaktifkan komputer, menghapus file, dll.

4. Ketentuan Hukum tentang Perlindungan Data di Indonesia

Di Indonesia pengaturan secara khusus mengenai perlindungan data memang belum ada, namun aspek perlindungannya sudah tercermin dalam peraturan perundang-undangan lainnya⁵⁸ seperti : UU No. 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan, UU No.8 Tahun 1997 tentang Dokumen Perusahaan, UU No. 7 Tahun 1992 jo UU No. 10 Tahun 1998 tentang Perbankan, UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 36 Tahun 2009 tentang Kesehatan dan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

a. Undang-Undang No. 7 Tahun 1971 tentang Ketentuan-Ketentuan Pokok Kearsipan

Undang-undang ini pada dasarnya mengatur aspek publik yaitu penyelenggaraan sistem kearsipan oleh pemerintah dalam rangka penyelenggaraan administrasi negara. Dalam sistem kearsipan ini dapat tercakup juga dan/atau informasi pribadi seseorang. Dalam UU ini terdapat ketentuan bahwa arsip dapat dirupakan dalam “bentuk corak apapun”, maka dalam hal ini dapat termasuk pula data elektronik. Mengenai keamanan data, UU ini mencantumkan ancaman pidana terhadap siapa saja yang memiliki secara melawan hukum dan/atau menyimpan dan dengan sengaja memberitahukan hal-hal tentang isi arsip tersebut pada pihak ketiga yang tidak mengetahui⁵⁹

⁵⁸Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, PT. Raja Grafindo Persada, Jakarta, 2005, hlm 177.

⁵⁹Edmon Makarim, *Ibid*, hlm 178.

b. Undang-Undang No. 8 Tahun 1997 tentang Dokumen Perusahaan

Melengkapi ketentuan mengenai Pokok Kearsipan yang lebih banyak mengatur aspek publik, maka dalam lingkup perusahaan diatur lebih lanjut dalam UU No. 8 Tahun 1997 tentang Dokumen Perusahaan⁶⁰. Dalam pasal 1, Dokumen Perusahaan didefinisikan sebagai data, catatan dan atau keterangan yang dibuat atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya baik tertulis di atas kertas atau sarana lain maupun te rekam dalam bentuk corak apapun yang dapat dilihat, dibaca atau didengar.

c. Undang-Undang No. 7 Tahun 1992 jo Undang-Undang No. 10 Tahun 1998 tentang Perbankan

Ketentuan yang berkaitan dengan perlindungan data pribadi dalam Undang-Undang Perbankan berkenaan dengan masalah rahasia bank. Berdasarkan Pasal 40 Undang-Undang Nomor 10 Tahun 1998, bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A. Pasal-pasal pengecualian tersebut adalah apabila untuk kepentingan perpajakan, untuk penyelesaian piutang bank, untuk kepentingan peradilan dalam perkara pidana, serta atas permintaan, persetujuan atau kuasa dari nasabah penyimpan, di mana bank dapat

⁶⁰Edmon Makarim, *Ibid*, hlm 178.

melanggar ketentuan mengenai rahasia bank ini tentunya dengan prosedur-prosedur tertentu.⁶¹

d. Undang-Undang No. 43 Tahun 2009 tentang Kearsipan

Berbeda dengan undang-undang sebelumnya, undang-undang yang merupakan undang-undang pengganti ini kini mengatur tidak saja mengatur mengenai penyelenggaraan kearsipan di lingkungan pemerintah, namun juga penyelenggaraan sistem kearsipan oleh lembaga negara, pemerintah daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan serta lembaga kearsipan. Dalam sistem kearsipan ini dapat tercakup juga data dan/atau informasi pribadi seseorang.

Yang dimaksud dengan arsip disini adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi. Mengenai perlindungan data pribadi undangundang ini menyatakan bahwa lembaga kearsipan dan pencipta arsip dapat menutup akses atas arsip dengan alasan apabila arsip dibuka untuk umum salah satunya dapat mengungkapkan rahasia atau data pribadi.

Dalam undang-undang ini juga diatur mengenai keamanan data, yang mencantumkan ancaman pidana terhadap setiap orang yang dengan sengaja menyediakan arsip dinamis kepada pengguna arsip

⁶¹Edmon Makarim, *Ibid*, hlm 179.

yang tidak berhak. Dalam Pasal 1 undang-undang ini, dijelaskan beberapa jenis arsip, yaitu:

- a. Arsip dinamis adalah arsip yang digunakan secara langsung dalam kegiatan pencipta arsip dan disimpan selama jangka waktu tertentu.
- b. Arsip vital adalah arsip yang keberadaannya merupakan persyaratan dasar bagi kelangsungan operasional pencipta arsip, tidak dapat diperbarui, dan tidak tergantikan apabila rusak atau hilang.
- c. Arsip aktif adalah arsip yang frekuensi penggunaannya tinggi dan/atau terus menerus.
- d. Arsip inaktif adalah arsip yang frekuensi penggunaannya telah menurun.
- e. Arsip statis adalah arsip yang dihasilkan oleh pencipta arsip karena memiliki nilai guna kesejarahan, telah habis retensinya, dan berketerangan dipermanenkan yang telah diverifikasi baik secara langsung maupun tidak langsung oleh Arsip Nasional Republik Indonesia dan/atau lembaga kearsipan.
- f. Arsip terjaga adalah arsip negara yang berkaitan dengan keberadaan dan kelangsungan hidup bangsa dan negara yang harus dijaga keutuhan, keamanan, dan keselamatannya.
- g. Arsip umum adalah arsip yang tidak termasuk dalam kategori arsip terjaga.

Selanjutnya, dalam Pasal 3 dinyatakan bahwa tujuan kearsipan adalah antara lain untuk menjamin perlindungan kepentingan negara dan hak-hak keperdataan rakyat melalui pengelolaan dan pemanfaatan arsip yang autentik dan terpercaya serta menjamin keselamatan dan keamanan arsip sebagai bukti pertanggung jawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Kemudian juga disebutkan salah satu asas dalam ketentuan ini adalah asas keselamatan dan keamanan.

e. Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi

Menurut Peraturan Pemerintah Tahun 2000 tentang Penyelenggaraan Telekomunikasi yang merupakan peraturan pelaksana dari Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, internet dimasukkan ke dalam jenis jasa multimedia, yang diidentifikasi sebagai penyelenggara jasa telekomunikasi yang menawarkan layanan berbasis teknologi informasi.

Hal tersebut menunjukkan bahwa pengaturan internet termasuk ke dalam hukum telekomunikasi. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa hal yang berkenaan dengan kerahasiaan informasi. Antara lain dalam Pasal 22 dinyatakan bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau manipulasi: (a) akses ke jaringan telekomunikasi; dan/atau (b) akses ke jasa telekomunikasi; dan atau (c) akses ke jaringan telekomunikasi khusus. Bagi pelanggar ketentuan tersebut diancam

pidana penjara maksimal enam tahun dan/atau denda maksimal Rp600 juta. Selanjutnya, di dalam Pasal 40 dinyatakan bahwa setiap orang dilarang melakukan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apa pun. Bagi yang melanggar ketentuan tersebut, diancam pidana penjara maksimal 15 Tahun. Undang-Undang Telekomunikasi ini juga mengatur kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirimkan dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya (Pasal 42 ayat (1)). Bagi penyelenggara yang melanggar kewajiban tersebut diancam pidana penjara maksimal dua tahun dan atau denda maksimal Rp200 juta.

Namun, penyelenggara jasa telekomunikasi wajib merekam informasi yang diperlukan untuk keperluan proses peradilan pidana atas permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu, yaitu tindak pidana yang diancam dengan pidana penjara selama lima tahun ke atas, seumur hidup atau mati. Permintaan dapat juga diajukan penyidik⁶²

- f. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Kitab Undang-Undang Hukum Pidana Indonesia belum mengatur yurisdiksi hukum atas kejahatan di dunia siber sehingga akan

⁶²Edmon Makarim, *Ibid*, hlm 181.

berdampak terhadap perlindungan hak-hak pribadi (privacy right) seseorang⁶³. Di dalam dunia siber masalah perlindungan hak pribadi (privacy right) sangat erat kaitannya dengan perlindungan data pribadi seseorang (personal data) karena saat ini perkembangan teknologi dalam dunia internet telah mengalami kemajuan yang sangat pesat sehingga orang dapat mengakses data-data pribadi seseorang tanpa sepengetahuan pihak yang bersangkutan⁶⁴. Sehingga kemungkinan terjadi pelanggaran terhadap hak pribadi seseorang sangat besar.

Salah satu hal yang menarik dalam Undang-Undang ini adalah bahwa dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi. Hal ini dinyatakan berdasarkan Pasal 9 bahwa Pelaku usaha yang menawarkan produk melalui sistem elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Selanjutnya Pasal 26 ayat (1) menyatakan kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang

⁶³Masalah hak cipta atas hasil karya di internet mencakup berbagai jenis pelanggaran yang biasanya dilakukan oleh para Hacker, Cracker, maupun Carder. Hacker adalah orang yang suka “memainkan” internet, menjelajahi ke situs internet orang lain dan perbuatannya disebut melakukan Hacking. Apabila Hacker menyusup dan menyelundup ke situs internet orang lain itu bersifat merusak disebut Cracker. Hacker yang menjelajahi berbagai situs dan “mengintip” data tetapi tidak merusak sistem komputer situs-situs orang atau lembaga lain, sering disebut Hecktivism. Kemudian dalam kejahatan siber, dikenal juga istilah Carder, yakni seorang yang menggunakan data kartu kredit milik orang lain untuk belanja lewat internet. Ahmad M. Ramli, *Perencanaan Pembangunan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi*. Badan Pembinaan Hukum Nasional Republik Indonesia, Jakarta, 2009. hlm 45.

⁶⁴Miller, Roger Leroy dan Jentz Gaylord, *Law for E-Commerce*, hlm 233

harus dilakukan atas persetujuan Orang yang bersangkutan. Ayat (2) kemudian menyatakan setiap orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini. Penjelasan Pasal 26 Ayat (1) menerangkan bahwa dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:

- a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
- b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
- c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang

Perlindungan data pada Pasal 26 ini adalah perlindungan mendasar terhadap privasi dan data. Dalam ketentuan ini perlindungan

data memuat unsur-unsur mengenai perlindungan terhadap privasi secara minimal dan sangat luas⁶⁵. Bagaimanapun juga, apabila ditarik penafsiran secara general terhadap perlindungan data, maka perlindungan data secara spesifik sebenarnya telah diatur ke dalam pasal-pasal selanjutnya, yaitu pada Pasal 30 sampai Pasal 33 dan juga

⁶⁵Dionysius Damas Pradiptya, "Pengaturan Perlindungan Data di Indonesia," Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (<http://indocyberlaw.org/?p=313>) Diakses pada 11 Februari 2019

pada Pasal 35 yang masuk ke dalam BAB VII mengenai Perbuatan Yang Dilarang. Dengan penggunaan tafsiran yang umum, pelanggaran terhadap perlindungan data dapat didasarkan pada ketentuan tersebut.

UU ITE sebenarnya secara komprehensif telah memuat ketentuan yang mengatur bagaimana perlindungan data diberikan kepada individu, badan hukum, dan pemerintah. Secara tegas UU ITE melarang adanya akses secara melawan hukum kepada data milik Orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengaman. Selain itu juga secara tegas UU ITE menyatakan bahwa penyadapan (interception) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam rangka upaya hukum⁶⁶. Berdasarkan UU ITE ini juga, setiap orang dilarang dengan cara apapun untuk membuka informasi milik orang lain dengan tujuan apapun bahkan jika data yang sifatnya rahasia sampai dapat terbuka kepada publik. Lebih jauh, perlindungan terhadap data tidak hanya mengatur akses pembukaan data saja, tetapi juga apabila data dapat dibuka dan diubah dengan cara apapun (manipulasi, perubahan, penghilangan, pengrusakan) sehingga seolah-olah data tersebut menjadi data otentik.

⁶⁶Dionysisus Damas Pradiptya, *Ibid.*,

Terlepas dari perbuatan yang terkait secara langsung dengan akses tanpa hak kepada data (unlawful access), UU ITE juga menyatakan melarang setiap tindakan yang mengakibatkan sistem elektronik menjadi terganggu yang secara sistematis berarti juga dapat mengakibatkan terganggunya akses data bagi pemiliknya. Perlindungan data disini tidak hanya pada terbebasnya data untuk terbuka dengan cara dan tujuan apapun tanpa persetujuan pemilik data saja, namun perlindungan data juga berarti pengamanan terhadap sistem elektronik dimana data disimpan dan digunakan untuk dapat berjalan sebagaimana mestinya. Dengan demikian melindungi sistem elektronik juga berarti melindungi data itu sendiri.⁶⁷

5. Perlindungan Data Pribadi dalam Beberapa Sistem Hukum

Di beberapa negara maju, masalah perlindungan data pribadi sudah dianggap sebagai bagian dari hak asasi manusia yang harus dilindungi dan oleh karenanya telah dituangkan dalam peraturan perundangan tersendiri. Eropa misalnya, sudah memiliki peraturan tentang perlindungan data pribadi selama lebih dari satu dekade.⁶⁸ Dalam penelitian ini akan diberikan tiga contoh negara maju yang telah memiliki pengaturan yang komprehensif terkait perlindungan data pribadi.

Inggris mengatur tentang perlindungan data pribadi dalam Data Protection Act 1998 yang mulai berlaku sejak tahun 2000. Act ini

⁶⁷Dionysisus Damas Pradiptya, *Ibid*.

⁶⁸Rosalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya", *Jurnal Hukum*, Edisi No. 2 Vol. 3, Fakultas Hukum Universitas Pelita Harapan Surabaya, 2014, hlm. 18.

merupakan pengganti dari peraturan sebelumnya (Data Protection Act 1984). Di Inggris terdapat suatu badan pelaksana yaitu The Data Protection Commisioner yang bertugas mengawasi semua pengguna data yang menguasai data pribadi. Perlindungan terhadap hak privasi individual dibuktikan dalam ketentuan Data Protection Act 1998 yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.⁶⁹ Data juga hanya boleh digunakan sepanjang diperlukan dan tidak boleh disimpan lebih lama dari seharusnya. Begitu kuatnya perlindungan terhadap data pribadi, Act ini bahkan melarang data pribadi ditransfer ke negara di luar Eropa kecuali apabila negara yang bersangkutan dapat menjamin perlindungan data yang serupa.

Beberapa prinsip penting dari Data Protection Act adalah sebagai berikut⁷⁰:

- 1) *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.* (Data pribadi akan diperoleh hanya untuk satu atau lebih tujuan yang ditentukan dan sah, dan tidak akan diproses lebih lanjut dengan cara apa pun yang tidak sesuai dengan tujuan itu atau tujuan itu.)
- 2) *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.* (Data pribadi yang diproses untuk tujuan atau tujuan apa pun tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan itu atau tujuan itu.)

⁶⁹Edmon Makarim, *Op. Cit*, hlm. 170

⁷⁰Rosalinda Elsina Latumahina, *Op. Cit*, hlm. 19.

- 3) *Personal data shall be processed in accordance with the rights of data subjects under this Act.* (Data pribadi akan diproses sesuai dengan hak-hak subyek data berdasarkan Undang-Undang ini.)
- 4) *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.* (Tindakan teknis dan organisasional yang tepat harus diambil terhadap pemrosesan data pribadi yang tidak sah atau melanggar hukum dan terhadap kehilangan atau kerusakan yang tidak disengaja dari, atau kerusakan pada, data pribadi.)
- 5) *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.* (Data pribadi tidak boleh ditransfer ke suatu negara atau wilayah di luar Wilayah Ekonomi Eropa kecuali jika negara atau wilayah itu memastikan tingkat perlindungan yang memadai untuk hak dan kebebasan subyek data dalam kaitannya dengan pemrosesan data pribadi.)

Malaysia maupun Singapura juga telah mengatur mengenai perlindungan data pribadi dalam perundangan tersendiri. Malaysia mengaturnya dalam Personal Data Protection Act (PDPA) 2010, sementara Singapura mengaturnya dalam Personal Data Protection Act (PDPA) 2012.⁷¹ PDPA 2010 milik Malaysia baru akan berlaku secara

penyempurnaan per Agustus 2013, sedangkan PDPA 2012 milik Singapura baru berlaku secara penuh pada bulan Juli 2014. Kedua aturan milik Malaysia dan Singapura ini mempunyai banyak kemiripan karena tampaknya mempunyai sumber yang sama, yaitu mengacu pada aturan tentang perlindungan data pribadi yang dianut di Eropa (European Data Protective Directive). Perbedaan yang menarik dari PDPA 2012 yang dimiliki

⁷¹Rosalinda Elsina Latumahina, Op. Cit, hlm. 19.

Singapura adalah bahwa PDPA 2012 ini memfasilitasi berdirinya sebuah badan bernama Do Not Call (DNC) Registry. Masyarakat dapat mendaftarkan nomor teleponnya pada DNC Registry dan secara resmi menolak untuk menerima telepon maupun pesan-pesan seperti SMS dan MMS dari marketing atau organisasi yang tidak dikehendakinya.⁷²

Karena terdapat kemiripan, maka dalam penelitian ini hanya akan dibahas salah satu Act secara garis besar, yaitu PDPA 2010 milik Malaysia. Sejak adanya PDPA 2010 tersebut, setiap orang akan mendapat hak-hak baru seperti hak untuk diinformasikan mengenai data pribadinya serta hak untuk mengakses, mengkoreksi dan juga mengontrol pengolahan atau penggunaan data pribadi mereka oleh pihak lain. Transfer data pribadi lintas batas (cross-border transfer) juga diatur dalam PDPA. PDPA menetapkan bahwa tidak ada transfer data pribadi di luar Malaysia dapat terjadi kecuali pada tempat yang telah ditetapkan oleh Menteri Informasi, Kebudayaan dan Komunikasi. Kemudian negara tujuan tempat data pribadi ditransfer wajib memiliki tingkat perlindungan yang memadai yang setidaknya setara dengan tingkat perlindungan yang diberikan oleh PDPA.

PDPA 2010 memuat tujuh prinsip hukum setiap pengguna data, sebagaimana diuraikan sebagai berikut; *The Malaysian PDPA requires users of data to comply with a number of principles, the General Principle,*

⁷²(<https://www.pdpc.gov.sg/legislation-andguide-lines/overview>) diakses pada 15 Februari 2019 pada pukul 08.45 WIB

the justification for the processing, such as consent; the Notice and Choice Principle, the right to be informed about the purposes for the processing; the Disclosure Principle, no disclosure except in connection with the purpose; the Security Principle, the obligation to take practical steps to protect data; Retention Principle, not to keep the data for longer than necessary; Data Integrity Principle, ensure that data is accurate and up to date; and the Access Principle, an individuals right to have access to his or her data. (PDPA Malaysia mewajibkan pengguna data untuk mematuhi sejumlah prinsip, Prinsip Umum, pembenaran untuk pemrosesan, seperti persetujuan; Prinsip Pemberitahuan dan Pilihan, hak untuk diberi tahu tentang tujuan pemrosesan; Prinsip Pengungkapan, tidak ada pengungkapan kecuali sehubungan dengan tujuan; Prinsip Keamanan, kewajiban untuk mengambil langkah-langkah praktis untuk melindungi data; Prinsip Retensi, tidak menyimpan data lebih lama dari yang diperlukan; Prinsip Integritas Data, memastikan bahwa data itu akurat dan terkini; dan Prinsip Akses, hak individu untuk memiliki akses ke datanya.)⁷³

Ketujuh prinsip ini sudah mengatur secara komprehensif mengenai perlindungan data pribadi. Dalam Retention Principle misalnya, data pribadi yang diproses untuk tujuan apapun harus tidak disimpan lebih lama dari yang diperlukan untuk pemenuhan tujuan perlindungan data pribadi. Dalam hal ini akan menjadi tugas dari pengguna data untuk mengambil

⁷³Rosalinda Elsina Latumahina, *Op. Cit*, hlm. 19.

semua langkah-langkah yang wajar untuk memastikan bahwa semua data pribadi dihancurkan atau dihapus secara permanen. Dengan adanya PDPA 2010 ini, jaminan keamanan bagi data pribadi pengguna internet di Malaysia pun meningkat.

B. Tinjauan Umum tentang Tanggung Jawab Penyedia Layanan atas Kerahasiaan Data Pribadi

1. Pengertian Tanggung Jawab dan Batas-Batasnya

Secara umum tanggung jawab dapat dibedakan dalam hukum perdata berdasarkan hukum perikatan, yaitu: (a) tanggung jawab hukum karena perjanjian/hubungan kontraktual (*privity of contract*) seperti yang tercantum dalam pasal 1338 dan pasal 1317 KUH Perdata, (b) tanggung jawab karena undang-undang. Adapun tanggung jawab yang lahir karena undang-undang meliputi dua hal yaitu tanggung jawab yang timbul karena UU saja dan tanggung jawab yang lahir sebagai akibat dari perbuatan orang, dimana perbuatan tersebut dapat bersifat sesuai dengan hukum (perbuatan yang sah / halal) maupun perbuatan yang melawan hukum yang disebut juga dengan istilah Perbuatan Melawan Hukum (PMH). Akan tetapi terdapat tanggung jawab yang tidak berakibat dari perbuatannya sendiri, melainkan akibat dari perbuatan orang atau benda yang berada dibawah kekuasaannya. Seperti yang tercantum dalam pasal 1367 KUH Perdata. Konsekuensi logisnya adalah mendapatkan perlindungan hukum atau upaya terbaiknya dalam bentuk terhindarnya mereka dari pola tanggung jawab yang bersifat mutlak (*strict liability*). Istilah “strict

liability” secara garis besar adalah tidak berbeda dengan absolute liability, yaitu pengertian yang sama dengan prinsip pertanggung jawaban mutlak. Perbedaan pokok antara strict liability bahwa perbuatan yang merugikan tersebut harus dilakukan oleh orang yang bertanggung jawab dengan absolute liability ada atau tidak adanya hubungan kausalitas antara kerugian dan pelaku tidak dipersyaratkan. Karena faktor-faktor yang biasanya dapat digunakan sebagai alasan untuk membebaskan suatu tanggung jawab menjadi tidak berlaku, kecuali dinyatakan secara khusus dalam undang-undang. Kasus hukum tentang penerapan teknologi informasi, bukan perbuatan yang dikenai perbuatan melawan hukum, tetapi cukup merupakan tindakan yang didasarkan pada kontrak saja atau tanggung jawab kontraktual. Karena berdasarkan kontrak yang dibuat adalah berdasarkan kesepakatan kedua belah pihak, dimana kuncinya adalah azas kebebasan berkontrak.

Pada dasarnya prinsip pertanggung jawaban hukum yang berlaku terhadap pelaku usaha adalah prinsip praduga tidak bersalah (presumed liability). Sedangkan dalam system hukum nasional sebagai konsekuensi dari pasal 1367 KUHPerdara yang menyatakan bahwa setiap orang harus bertanggung jawab atas orang atau benda yang berada dibawah penguasaannya. Pada pasal 17(1) UU ITE disebutkan bahwa para pihak wajib beritikad baik, Sehingga penerapan strict liability harus dilihat terhadap kasus-kasus tertentu agar tidak terjadi kerugian pada pihak lain. Dalam pasal (18) UU ITE dinyatakan bahwa transaksi elektronik

dituangkan kedalam kontrak elektronik yang mengikat kedua belah pihak.⁷⁴

2. Surat Elektronik

Surat adalah suatu sarana untuk menyampaikan informasi atau pernyataan secara tertulis kepada pihak lain baik itu atas nama sendiri ataupun atas nama jabatannya di dalam organisasi.⁷⁵ Sedangkan terdapat pendapat lain surat adalah suatu alat komunikasi yang mana pihak yang satu ingin menyampaikan maksud kepada pihak lain secara tertulis.⁷⁶

Selain pendapat di atas, terdapat pengertian surat yang lainnya yaitu surat adalah penyampaian informasi secara tertulis dari satu pihak ke pihak lain berupa pemberitahuan, pernyataan, permintaan, laporan, pertanyaan, pemikiran, pemikiran, sanggahan, kritikan, dan sebagainya.⁷⁷ Berdasarkan pengertian-pengertian tersebut di atas maka dapat disimpulkan bahwa surat merupakan alat komunikasi tertulis yang digunakan untuk menyampaikan informasi dari pihak yang satu kepada pihak lain. Dari pengertian tersebut pula dapat diketahui bahwa terdapat dua pihak yang terlibat dengan surat yakni pengirim dan penerima surat. Apabila pengirim dan penerima surat menjalin hubungan secara berkesinambungan maka terjadilah aktivitas surat menyurat. Surat menyurat dapat diartikan sebagai

⁷⁴Nining Latianingsih, "Prinsip Tanggung Jawab Pelaku Usaha dalam Transaksi Elektronik Menurut Undang-Undang Informasi dan Transaksi Elektronik", *Jurnal Ekonomi dan Bisnis* Vol. 11 No. 2, Politeknik Negeri Jakarta, 2012, hlm. 75.

⁷⁵Djihad Hisyam, "Korespondensi Bahasa Indonesia dalam Teori dan Praktik", *Skripsi*, Yogyakarta, Universitas Negeri Yogyakarta, 2008, hlm 2

⁷⁶Wasiti, "English correspondence practice", *Skripsi*, Yogyakarta, Universitas Negeri Yogyakarta, 2010, hlm 1

⁷⁷Sutrisno & Lijah Tjarlisjasih, *Melakukan Prosedur Administrasi*, Yudhistira, Bandung, 2007, hlm 6

suatu kegiatan pengendalian arus berita tertulis yang timbul dari adanya suatu pencatatan, laporan atau keputusan yang memungkinkan terjadinya permintaan, pemberitahuan, dan sebagainya.⁷⁸ Kegiatan surat menyurat dapat terjadi apabila pihak penerima surat memberikan jawaban terhadap surat yang telah dikirim oleh pihak pengirim surat.

3. Pengertian Surat Elektronik (e-mail)

Surat merupakan alat komunikasi tertulis yang digunakan untuk menyampaikan pesan atau informasi dari pihak yang satu kepada pihak lainnya. Di era sebelum teknologi berkembang pesat, organisasi atau instansi pada umumnya masih menggunakan surat tercetak. Akan tetapi, seiring berjalannya waktu surat telah mengalami perkembangan mengikuti arus teknologi yang semakin pesat yakni dengan menggunakan surat tidak tercetak. Surat tidak tercetak tersebut disebut pula dengan surat elektronik (e-mail).

Surat elektronik atau electronic mail (e-mail) adalah salah satu bentuk atau cara pengiriman surat, informasi, atau pesan (bisnis dan nonbisnis) yang dilakukan secara elektronik, tanpa kertas, dan tanpa jasa pengirim.⁷⁹ Terdapat pengertian lain yaitu surat elektronik didefinisikan sebagai komunikasi pesan nonverbal dari seseorang ke orang lain dengan memakai media penyampaian (transmission) elektronik.⁸⁰

⁷⁸Tintin Astini, dan Aah Johariah, *Melakukan Prosedur Administrasi*, Armico, Bandung, 2004, hlm 19

⁷⁹Djoko Purwanto, *Korespondensi Bisnis Modern*, Esensi Erlangga Group, Jakarta, 2007, hlm 170

⁸⁰Stallord, John J, *Perkantoran Elektronik*, Rineka Cipta, Jakarta, 1990, hlm 118

Selain pendapat di atas, terdapat pengertian lain yaitu surat elektronik (disingkat ratel atau surel atau surat-e) atau pos 10 elektronik (disingkat pos-el) atau nama umumnya dalam Bahasa Inggris e-mail atau email adalah sarana kirim mengirim surat melalui jalur internet.⁸¹ Berdasarkan definisi yang telah dikemukakan oleh beberapa penulis di atas dapat disimpulkan bahwa surat elektronik (e-mail) merupakan suatu metode pengiriman informasi atau pesan yang dikirim oleh pihak yang satu kepada beberapa pihak lainnya secara elektronik. Surat elektronik (e-mail) dapat pula disebut sebagai surat yang tidak tercetak atau tidak menggunakan kertas serta di dalam pengirimannya memerlukan adanya jaringan internet.

4. Sejarah Surat Elektronik (e-mail)

Sejarah surat elektronik (e-mail) dimulai pada tahun 1968, perusahaan yang bernama Olt Break and Newman (BNN) dikontrak oleh Departemen Pertahanan Amerika Serikat untuk menciptakan sesuatu yang disebut ARPANET yang kemudian berubah menjadi Internet. ARPANET merupakan singkatan dari Advanced Research Projects Agency Network yang dibentuk dengan tujuan untuk menciptakan sebuah metode komunikasi antara institusi militer dengan institusi pendidikan.

Pada tahun 1971, seorang insinyur yang bernama Ray Tomlinson diberi tugas dalam proyek yang disebut dengan SNDMSG. SNDMSG merupakan suatu program lama yang berfungsi untuk mengirimkan pesan

⁸¹Yanto Yulianto, *Pengertian dan Cara Pengelolaan Email dan Grup*, (<http://yantoyulianto.blogspot.com/2011/04/pengertian-dan-cara-pengelolaanemail.html>) diakses tanggal 27 Februari 2019.

ke dalam kotak surat pada mesin yang sama. Sehingga apabila seseorang telah membuat pesan dan memasukkannya pada kotak surat mesin tersebut maka orang lain yang menggunakan mesin atau komputer tersebut dapat membaca isi pesan yang terdapat pada kotak suara di komputer yang bersangkutan.

Pada awalnya Ray Tomlinson bereksperimen dengan program SNDMSG tersebut kemudian melanjutkan eksperimennya dengan menggunakan file protocol yang bernama CYPNET. File protocol CYPNET ini digunakan sebagai pendukung program SNDMSG agar dapat mengirimkan pesan ke komputer lain yang masih berada dalam jaringan ARPANET.

Pada tahun 1972, Ray Tomlinson mengenalkan ikon “@” (at) yang berarti pada, sebagai identitas e-mail untuk memisahkan antara user id dan domain pada sebuah alamat e-mail. Salah satu program e-mail pertama yang terbesar dan dapat digunakan secara umum adalah Eudora. E-mail tersebut pertama kali ditulis pada tahun 1988 oleh Steve Dorner seorang karyawan di University of Illionis.⁸²

5. Fungsi Surat Elektronik (e-mail)

Surat elektronik (e-mail) memiliki beberapa fungsi bagi penggunanya. E-mail memiliki beberapa fungsi dasar dan beberapa fungsi tambahan bagi penggunanya, diantaranya⁸³:

⁸²(www.asalusul.com/2009.02/sejarah-dan-seluk-beluk-surat-1428.html?m=1) diakses tanggal 27 Februari 2019.

⁸³Djoko Purwanto, Op. Cit, hlm 177

1. Fungsi dasar e-mail, antara lain:

- 1) Menerima pesan e-mail;
- 2) Membaca pesan e-mail;
- 3) Mengirim pesan e-mail;
- 4) Menjawab pesan e-mail yang masuk;
- 5) Meneruskan pesan e-mail yang masuk ke pemakai lain.

2. Fungsi tambahan e-mail, antara lain:

- 1) Menyimpan pesan yang telah dikirim;
- 2) Menyimpan pesan yang telah diterima dan dibaca;
- 3) Mengelola daftar alamat e-mail;
- 4) Menambahkan file untuk pesan yang akan dikirim;
- 5) Memisahkan file dari pesan yang masuk.

Surat elektronik memiliki beberapa fungsi bagi penggunanya dan memudahkan pengguna dalam menggunakan surat elektronik. Selain itu, fungsi-fungsi yang terdapat dalam surat elektronik dapat digunakan untuk menyelesaikan kegiatan surat elektronik secara cepat dan lancar.

C. Tinjauan Umum Tentang Layanan Gmail

1. Pengertian Gmail

Gmail yakni kependekan dari Google Mail. Gmail / Google Mail yakni layanan surat elektronik (surel) berbasis web yang disediakan oleh Google, Inc secara gratis kepada semua orang (penggunanya). Layanan ini diluncurkan pada tanggal 21 Maret 2004 dan menyediakan kapasitas email

1 GB. Semua orang dapat menciptakan account gmail tanpa harus melalui undangan dari orang yang sebelumnya sudah mendapat account. Dewasa ini menciptakan account gmail merupakan sudah menjadi suatu keharusan bagi banyak orang, karena gmail merupakan surat elektronik terkemuka yang sangat diharapkan oleh banyak orang, baik itu untuk berkomunikasi maupun untuk banyak sekali keperluan lainnya.

2. Sejarah Terbentuknya Gmail

Gmail adalah layanan surel (surat elektronik) milik Google yang dibentuk oleh Paul Buchheit. Pengguna sanggup mengakses Gmail dalam bentuk surat web HTTPS,⁸⁴ protokol POP3,⁸⁵ ataupun IMAP4.⁸⁶ Gmail diluncurkan dengan sistem undangan dalam bentuk Beta pada 1 April 2004, dan tersedia untuk publik pada 7 Februari 2007 meski masih menyandang status Beta. Bersama seluruh produk Google Apps, layanan ini tidak lagi Beta pada 7 Juli 2009.

Dengan kapasitas penyimpanan awal 1 GB per pengguna, Gmail berhasil meningkatkan standar penyimpanan gratis surat web dari 2-4 MB yang ditawarkan para pesaingnya pada waktu itu. Pesan pribadi, termasuk lampiran, dibatasi hingga 25 MB, lebih besar daripada layanan surat web

⁸⁴HTTPS adalah singkatan dari hypertext transfer protocol secure merupakan suatu protokol komunikasi dalam jaringan internet. HTTPS dapat diartikan sebagai bentuk protokol internet yang paling valid dan yang paling aman. HTTPS ini akan melindungi integritas serta kerahasiaan antara situs dan komputer pengguna.

⁸⁵POP3 (*Post Office Protocol version 3*) adalah protokol yang digunakan untuk mengambil surat elektronik (email) dari server email.

⁸⁶IMAP (*Internet Message Access Protocol*) adalah protokol standar untuk mengakses/mengambil e-mail dari server. IMAP memungkinkan pengguna memilih pesan e-mail yang akan ia ambil, membuat folder di server, mencari pesan e-mail tertentu, bahkan menghapus pesan e-mail yang ada.

lainnya. Gmail mempunyai antarmuka berorientasi pencarian dan "tampilan percakapan" yang ibarat dengan forum Internet. Sejumlah pengembang web mengakui Gmail yakni layanan pertama yang menggunakan metode pemrograman Ajax. Gmail beroperasi dengan Google GFE/2.0 di Linux. Pada Juni 2012, Gmail yakni layanan surat elektronik berbasis web terbesar dengan 425 juta pengguna aktif di seluruh dunia.⁸⁷

3. Kegunaan Layanan Gmail

Gmail/Google mail mempunyai banyak fungsi/kegunaan bagi para penggunanya. Fungsi gmail bagi penggunanya antara lain, sebagai alat untuk berkomunikasi (surat-menyurat elektronik) dengan orang lain, sebagai alat yang diharapkan untuk menciptakan akun media umum ibarat facebook, twitter, linkedin, instagram, path, dan lainnya, sebagai alat yang diharapkan dalam menciptakan akun paypal (rekening online), sebagai alat yang diharapkan dalam berbisnis online, seperti menciptakan blog baik itu blogspot maupun wordpress, mendaftar di situs paid survey, maupun untuk mendaftar di situs paid to click (PTC). Pada satu perangkat yang telah terlogin akun Google maka di dalam perangkat tersebut akan terlogin juga pada aplikasi-aplikasi lain salah satunya adalah Gmail dan halaman Web pencarian Google. Disamping itu tentu gmail mempunyai banyak fungsi lainnya.

⁸⁷ <https://id.wikipedia.org/wiki/Gmail> diakses pada 7 Mei 2019 pukul 9. 15 WIB

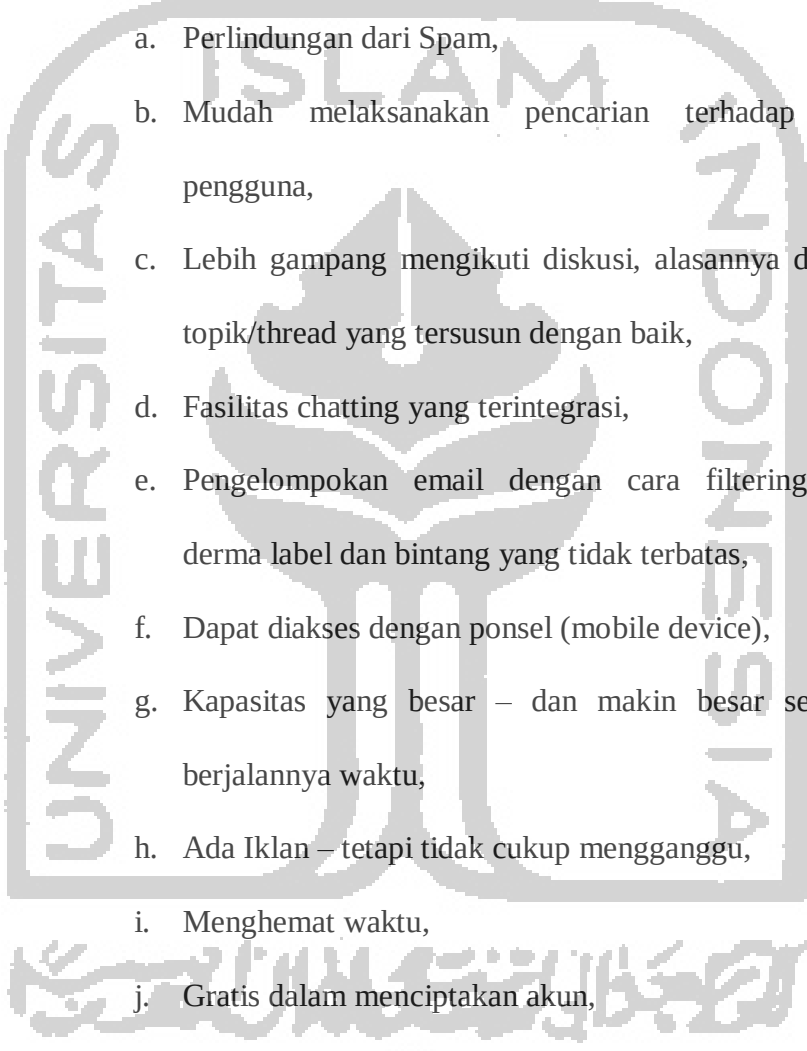
4. Fitur Layanan Gmail

Gmail menyediakan kapasitas penyimpanan sebanyak lebih dari 7538 megabyte dan terus bertambah. Jumlah ini lebih dari jumlah yang disediakan situs lain, seperti Yahoo! dan Hotmail. Hal ini berarti para pengguna sanggup menyimpan hingga ribuan surat elektronik. Sampai saat ini, gmail merupakan email dengan kapasitas terbanyak.

Gmail juga mengaplikasi teknologi pencarian Google yang memudahkan penggunanya mencari sesuatu dari email mereka. Gmail juga menampilkan iklan yang didasarkan dari email yang diterima pengguna. Iklan tersebut hanya diperlihatkan ke pengguna Gmail dan tidak dikirimkan ke alamat eksternal. Gmail sanggup mengirimkan lampiran hingga 25 MB per email. Gmail juga menawarkan layanan penyortiran email dalam bentuk "Conversation view". Dengan begini email yang diterima akan diurutkan dalam bentuk percakapan. Hal ini dapat mempermudah pengguna untuk melihat email yang mereka terima.

Gmail juga menyediakan layanan untuk melabeli email yang diterima pengguna. Satu email mampu mempunyai lebih dari satu label. Kegunaan dari fitur ini adalah untuk menyortir email sesuai dengan label yang diberikannya, Google juga dapat memperlihatkan label secara otomatis dengan sebuah filter. Teknologi Push e-mail juga diterapkan Gmail pada perangkat iPhone dan Windows Mobile, sedangkan pada perangkat Telepon pintar (smartphone) lainnya kemampuan teknologi Push e-mail dari Gmail ini bervariasi tergantung dari aplikasi yang bisa dipasang pada

Telepon dari banyak sekali brand dan jenis. Gmail juga mengaplikasi teknologi pencarian Google yang memudahkan penggunanya mencari sesuatu dari email mereka, terdapat 12 fitur unggulan dari layanan Gmail:⁸⁸

- 
- a. Perlindungan dari Spam,
 - b. Mudah melaksanakan pencarian terhadap email-email pengguna,
 - c. Lebih gampang mengikuti diskusi, alasannya dibantu layout topik/thread yang tersusun dengan baik,
 - d. Fasilitas chatting yang terintegrasi,
 - e. Pengelompokan email dengan cara filtering/penyaringan, derma label dan bintang yang tidak terbatas,
 - f. Dapat diakses dengan ponsel (mobile device),
 - g. Kapasitas yang besar – dan makin besar seiring dengan berjalannya waktu,
 - h. Ada Iklan – tetapi tidak cukup mengganggu,
 - i. Menghemat waktu,
 - j. Gratis dalam menciptakan akun,
 - k. Terintegrasi dengan seluruh produk Google.

⁸⁸<https://tarbiyahan.blogspot.com/2019/03/gmailapa-itu-gmaildan-bagaimana-sejarah.html> diakses pada 7 Mei 2017 pukul 9.33 WIB