UNIVERSITAS INDONESIA

ANALISIS YURIDIS MENGENAI PERLINDUNGAN DATA PRIBADI DALAM CLOUD COMPUTING SYSTEM DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

SKRIPSI

RADIAN ADI NUGRAHA
0806342983

FAKULTAS HUKUM
PROGRAM STUDI ILMU HUKUM
KEKHUSUAN HUKUM TENTANG KEGIATAN EKONOMI
DEPOK
JANUARI 2012

UNIVERSITAS INDONESIA

ANALISIS YURIDIS MENGENAI PERLINDUNGAN DATA PRIBADI DALAM CLOUD COMPUTING SYSTEM DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Indonesia

RADIAN ADI NUGRAHA
0806342983

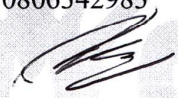
FAKULTAS HUKUM
PROGRAM STUDI ILMU HUKUM
KEKHUSUAN HUKUM TENTANG KEGIATAN EKONOMI
DEPOK
JANUARI 2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: Radian Adi Nugraha
NPM	: 0806342983
Tanda Tangan	: 
Tanggal	: 20 Januari 2012

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh

Nama	: Radian Adi Nugraha
NPM	: 0806342983
Program Studi	: Hukum
Judul Skripsi	: Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Hukum pada Progran Studi Reguler, Fakultas Hukum, Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Brian A. Prastyo, S.H., MLI	( )
Penguji	: Henny Marlyna, S.H., M.H., MLI	( )
Penguji	: Ranggalawe Suryasaladin, S.H., M.H., LL.M.	( )
Penguji	: Bono Budi Priambodo, S.H., M.Sc.	( )

Ditetapkan di : Depok

Tanggal : 20 Januari 2012

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi berjudul **"Analisis Yuridis Mengenai Perlindungan Data Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik".** Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Hukum pada Fakultas Hukum Universitas Indonesia. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkulihan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Brian A. Prastyo, S.H., M.LI , selaku Dosen Pembimbing dalam penulisan skripsi ini yang telah banyak memberikan kemudahan, arahan dan telah menyediakan waktu, tenaga serta pikiran untuk membimbing penulis dalam penyusunan skripsi ini. Dan juga member peluang bagi penulis untuk dapat juga berkontribusi dalam jurnal Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia dan mendalami hukum telematika di kampus FHUI ini.
2. Ibu Henny Marlyna, S.H., M.H., MLI, selaku Penguji dalam skripsi ini yang telah memberikan kritik dan saran bagi penulis.
3. Bapak Ranggalawe Suryasaladin, S.H., M.H., LL.M., selaku Penguji dalam skripsi ini yang telah memberikan kritik dan saran bagi penulis.
4. Bapak Bono Budi Priambodo, S.H., M.Sc, selaku Penguji dalam skripsi ini yang telah memberikan kritik dan saran bagi penulis.
5. Bapak M. Sofyan Pulungan, S.H., M.A, selaku Pembimbing Akademik penulis yang telah banyak memberi dukungan dan membantu penulis demi kelancaran studi di FHUI.
6. Ibu Myra R. Setiawan, S.H., M.H., selaku Sekretaris Bidang Studi Hukum Keperdataan yang telah menyetujui topik skripsi ini.

7. Bapak Ir. Tony Seno Hartono, selaku National Technology Officer Microsoft Indonesia yang telah berkenan menjawab pertanyaan penulis seputar komputasi awan.
8. Bapak Kurnia Wahyudi, S.Kom, selaku Country Manager for Cloud Computing IBM Indonesia yang telah berkenan menjawab pertanyaan penulis seputar komputasi awan.
9. Ibu Anggana Gunita, S.H., M.H., selaku Legal Officer Biznet Networks yang telah membantu penulis dalam usaha memperoleh data yang diperlukan sekaligus berkenan menjawab pertanyaan penulis dalam penyusunan skripsi ini.
10. Bapak Donny Budhiyo Utoyo, S.Kom, selaku Executive Director dari ICT Watch yang telah berkenan menjawab pertanyaan penulis seputar penerapan UU ITE dalam komputasi awan
11. Orang tua penulis, Bapak Ir. Nur Al Fata, M.T. dan Ibu Dra. Noor Salatiningsih, atas kasih sayang, dukungan, doa restu yang terus mengiringi bagi penulis hingga bisa meraih gelar sarjana. Skripsi ini Radian tujukan untuk Bapak dan Ibu semoga ilmu yang telah diperoleh selama ini bisa bermanfaat kedepannya dan menjadi aliran pahala yang tidak terputus untuk Bapak dan Ibu. Dan kepada ketiga adik penulis Amanda, Adeela dan Daanish semoga skripsi ini bisa memacu mencapai prestasi akademik dan non-akademik yang terbaik.
12. Para seluruh Pimpinan Fakultas, Pelaksana Akademik, Pelaksana Administrasi, Unit-Unit Kerja, dan staf pengajar Fakultas Hukum Universitas Indonesia
13. Pak Selam, Pak Indra dan segenap petugas Biro Pendidikan Fakultas Hukum Universitas Indonesia. Terima kasih untuk segala kesabaran dan kegigihan demi kelancaran studi mahasiswa.
14. Seluruh partner dalam Akademi Riset dan Kajian Hukum (ARKH) yaitu Fathan, Liza, Anto, Riko, Patra dan Femi yang telah bersama-sama meraih prestasi gemilang baik di tingkat nasional. Terima kasih atas kerjasamanya membawa ARKH meraih Juara 1 Environment Research Narration 2011 dan Juara II Contract Drafting Business Law Competition 2011

15. Segenap Badan Pengurus Harian Lembaga Kajian Keilmuan Fakultas Hukum Universitas Indonesia (LK2 FHUI) periode kepengurusan 2010 yaitu Anto, Femi, Rieya, Reza, Rantie, Fathan, Astri, Liza, Fadhil, Maria, Yella, Nessa, Ires, Ika, Najmu, Patra, Archie, dan Indri.
16. Seluruh jajaran Pengurus Indonesian Intellectual Property Academy yang telah memberikan pengalaman kerja yang berharga selama penulis menempuh studi di FHUI
17. Lembaga Bantuan Hukum Masyarakat dan para staf serta para volunteer, Pak Dhoho, Bang Tobas, Bang Ricky, Mbak Ajeng, Answer, Badar, Febri, Zacky, Fery, Alex, Obet, Tyo yang telah memberikan saya kesempatan untuk terjun langsung dalam advokasi hukum dan mengubah pola pikir saya sebagai mahasiswa hukum untuk lebih peduli terhadap kaum yang termajinalkan dan terdiskriminasi.
18. Teman-teman seperjuangan di FHUI angkatan 2008 yang tidak bisa disebutkan satu persatu. Sangat bangga bisa berada di tengah-tengah kalian.
19. Seluruh penghuni markas DO2A yaitu Faisal, Gede, Firman, Rangga, Ohiyong, Aldamayo, Umar, Bagus, Titan, Anandito dan M. Rizaldi. Semoga kita bisa berkumpul dan bermain bersama kembali
20. Sir Timothy John Berners-Lee atas temuannya yang mengubah dunia yaitu internet. Tanpa adanya internet, niscaya skripsi saya bertema komputasi awan ini tidak akan pernah akan terwujud.
21. Larry Page dan Sergey Brin, selaku pendiri *Google Corp* dengan segala kecanggihan mesin pencari dan software pendukung yang sangat membantu penulis menemukan data yang diperlukan di dunia maya.
22. Para senior dan junior penulis selama menempuh studi di FHUI
23. Dan semua pihak yang tidak dapat penulis satu persatu

Depok, 20 Januari 2012

Radian Adi Nugraha

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Radian Adi Nugraha
NPM	: 0806342983
Fakultas	: Hukum
Jenis Karya	: Skripsi

Demi kepentingan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Nonekslusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Nonekslusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta sebagai pemilik hak cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada Tanggal : 20 Januari 2012

Yang menyatakan

(Radian Adi Nugraha)

ABSTRAK

Nama : Radian Adi Nugraha

Program Studi : Hukum

Judul Skripsi : Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik

Skripsi ini membahas mengenai penerapan pasal perlindungan data pribadi yang terdapat dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dikaitkan dengan praktik layanan komputasi awan yang saat ini sedang berkembang pesat. Kebutuhan komputasi awan diperkirakan akan mengalami peningkatan yang sangat besar di masa mendatang. Hal tersebut didorong makin banyaknya penggunaan perangkat yang terhubung ke internet dan membutuhkan akses layanan berbasis data secara *real time*. Sebagai sebuah jenis layanan yang masih tergolong baru di Indonesia, isu keamanan dan perlindungan data pribadi dinilai masih menjadi poin penting yang dikhawatirkan dalam adopsi komputasi awan di Indonesia, menyusul banyaknya kasus pembobolan data yang merugikan pengguna layanan berbasis media elektronik seperti telepon selular dan kartu kredit. Dalam penelitian ini akan dibahas mengenai konsep umum perlindungan data, peraturan perundang-undangan yang mengatur tentang perlindungan data baik di dalam maupun luar negeri, tinjauan umum dari komputasi awan, analisis pasal 26 UU ITE dan tanggung jawab dari penyedia layanan komputasi awan terhadap data pribadi pengguna layanannya.

Kata Kunci : Perlindungan Data Pribadi, Privasi, Komputasi Awan

ABSTRACT

Name : Radian Adi Nugraha

Major : Law

Title : Juridical Analysis Concerning the Personal Data Protection In The Cloud Computing System from the Law of Information and Electronic Transactions

This paper discusses around the application of article about personal data protection that contained in Law No. 11 Year 2008 on Information and Electronic Transaction associated with the practice of cloud computing service that is growing rapidly nowadays. The need of cloud computing are predicted to get a huge increase in the future. It is driven more and more use of the devices that connected to the internet and require access to data-based services in real time. As a kind of the new service in Indonesia, the issue of security and personal data protection is still considered to be an important point of concern in the adoption of cloud computing in Indonesia, following a number of data leaked cases that adverse subject data of electronic media-based services such as mobile phones and credit cards. In this study will be discussed on the general concept of data protection, laws and regulations governing data protection both inside and outside the country, an overview of cloud computing, analysis of article 26 of Law of Information and Electroninc Transactions and responsibilities of providers of cloud computing services to the user's personal data from its services.

Key Words : Personal Data Protection, Privacy, Cloud Computing

.

DAFTAR ISI

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi kini sangat cepat dan jauh berbeda dengan masa awal kehadirannya. Era globalisasi telah menempatkan peranan teknologi informasi ke dalam suatu posisi yang sangat strategis karena dapat menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu serta dapat meningkatkan produktivitas serta efisiensi. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung secara cepat dengan signifikan.

Tak dapat disangkal bahwa perkembangan teknologi informasi dan komunikasi yang demikian pesat ikut mengubah sikap dan perilaku masyarakat dalam komunikasi dan interaksi. Hampir seluruh aspek kehidupan masyarakat selalu bersentuhan langsung dengan teknologi dan terbukti mendatangkan manfaat bagi perkembangan dan peradaban manusia. Kemajuan teknologi menghasilkan sejumlah situasi yang tak pernah terpikirkan sebelumnya oleh manusia[1]. Perkembangan teknologi yang demikian cepat, khususnya pada dunia perkomputeran, telah memberikan banyak kemudahan bagi manusia dalam melakukan setiap pekerjaan. Kemajuan yang diraih selalu berjalan beriring antara software atau perangkat lunak dengan hardwarenya atau perangkat keras.

Teknologi informasi mencakup sistem yang mengumpulkan (*collect*), menyimpan (*store*), memproses, memproduksi dan mengirim informasi dari dan ke industri ataupun masyarakat secara efektif dan cepat. Kini sistem informasi dan komunikasi elektronik telah diimplementasikan pada hampir semua sektor kehidupan dalam masyarakat yang akhirnya juga mengakibatkan terciptanya suatu pasar baru yang telah mendorong perkembangan sistem ekonomi masyarakat dari traditional ekonomi yang berbasiskan industri manufaktur ke arah *digital economy* yang berbasiskan informasi, kreatifitas intelektual dan ilmu pengetahuan yang

[1] Diaz Gwijangge, "Peran TIK Dalam Pembangunan Karakter Bangsa," (makalah Disampaikan dalam Workshop: "Pemanfaatan Jejaring E-Pendidikan" yang diselenggarakan Pusat Teknologi Informasi dan Komunikasi Pendidikan Kementerian Pendidikan Nasional, Sulawesi Selatan, 14 Juni 2011), hlm. 1

juga dikenal dengan istilah *Creative Economy*[2]. Perkembangan teknologi informasi dapat meningkatkan kinerja dan memungkinkan berbagai kegiatan dapat dilaksanakan dengan cepat, tepat dan akurat, sehingga akhirnya akan meningkatkan produktivitas. Perkembangan teknologi informasi memperlihatkan bermunculannya berbagai jenis kegiatan yang berbasis pada teknologi ini, seperti *e-government*[3], *e-commerce*[4], *e-education*[5], *e-medicine*, *e-laboratory*, dan lainnya, yang kesemuanya itu berbasiskan elektronika[6]. Kehadirannya telah membentuk dunia tersendiri yang dikenal dengan dunia maya (*Cyberspace*) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk *virtual* (tidak langsung dan tidak nyata).

Saat ini dengan cepatnya perkembangan teknologi informasi telah membuat proses dan strategis bisnis berubah dengan cepat. Tidak ada lagi manajemen perusahaan yang tidak peduli dengan persaingan produk dari rival bisnisnya, Penggunaan perangkat teknologi informasi sudah menjadi keharusan saat ini, yang dapat dilihat dari anggaran belanja sampai dengan implementasi teknologi informasi di sebuah perusahaan. Teknologi informasi sudah dipandang sebagai salah satu senjata untuk bersaing di kompetisi global, kecenderungan ini terlihat dari tidak digunakannya lagi teknologi informasi sebagai pelengkap dari

[2]Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, (Jakarta: Raja Grafindo Persada, 2010), hlm. 2.

[3] Definisi E-Government menurut United Nations Online Network in Public Administration and Finance adalah mendayagunakan internet dan *world wide web* untuk memberikan informasi dan layanan dari pemerintah kepada warga negara

[4] Definisi E-Commerce dari Electronic Cornmerce Expert Group (ECEG) Australiaadalah *Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, Internet and the telephone*

[5] E-education merupakan pengembangan sarana pendidikan secara elektronik yang memungkinkan proses belajar mengajar secara jarak jauh (e-learning). Diharapkan akan terbuka kesempatan pemerataan pendidikan dengan kualitas yang sama dengan pendidikan formal

[6] Wawan Wardiana, "Perkembangan Teknologi Informasi di Indonesia". (makalah disampaikan dalam Seminar dan Pameran Teknologi Informasi 2002, Fakultas Teknik Universitas Komputer Indonesia (UNIKOM) Jurusan Teknik Informatika, tanggal 9 Juli 2002) Hlm 1

proses bisnis perusahaan, namun teknologi informasi dijadikan sebagai bagian dari proses bisnisnya[7]

Kebutuhan komputasi awan diperkirakan bakal mengalami peningkatan yang sangat besar di masa mendatang. Hal tersebut didorong makin banyaknya penggunaan perangkat yang terhubung ke internet dan membutuhkan akses layanan berbasis data secara *real time*[8]. Nick Knupffer, *Marketing Director Data Center* dan *Connected System* Group APAC, PRC Intel di Jakarta mengungkapkan bahwa pada tahun 2015, lebih dari 2,5 miliar orang akan menggunakan 15 miliar perangkat yang terhubung dengan internet, lebih dari kebutuhan yang diakses saat ini. Pada tahun 2015 tersebut, trafik internet bisa mencapai hingga ukuran zetabyte atau miliar miliar juta bytes[9]

Komputasi awan memang menjadi bisnis yang diminati dan diproyeksikan akan terus berkembang. Cisco Internet Business Solutions Group (CIBSG) belum lama ini mengemukakan hasil risetnya mengenai potensi *cloud computing*. Perkiraannya, pendapatan yang bisa diperoleh dari bisnis komputasi awan di dunia bisa mencapai US$ 44 miliar pada tahun 2013[10]. Komputasi Awan nampaknya akan mencerminkan dunia komputer saat ini, dan banyak ahli yang percaya sekarang bahwa komputasi awan akan menjadi "*The Next Big Thing*"[11]

Pasar cloud Indonesia dinilai tengah berada dalam kurva pertumbuhan pesat dan semakin banyak perusahaan yang akan menjadikan cloud sebagai prioritas mereka dalam tahun-tahun mendatang[12]. Hal ini didorong oleh fakta

---

[7] Deris Setiawan. Mengenal Cloud Computing. <http://deris.unsri.ac.id/materi/jarkom/mengenal_cloudcomputing.pdf>Hlm .1

[8] Kampanyekan Cloud Dengan Solusi Satu Kotak. <http://tekno.kompas.com/read/2011/09/12/2144062/Kampanyekan.Cloud.dengan.Solusi.Satu.Kotak> Diakses pada 13 September 2011

[9] Ibid.

[10] Cisco: Pendapatan dari Public Cloud Computing Dunia diperkirakan US$44 M di 2013. <http://www.wartaekonomi.co.id/berita-115429668-cisco-pendapatan-dari-public-cloud-computing-dunia-diperkirakan-us44-m-di-2013.html.>Diakses pada 22 Agustus 2011

[11] David C. Wyld, "The Cloudy Future of Government IT : Cloud Computing and The Public Sector Around The World," International Journal of Web & Semantic Technology (IJWesT), Vol 1, (January 2010), hlm. 1.

[12] Pasar Komputasi Awan Tumbuh 53,4%, <http://www.bisnis.com/articles/pasar-komputasi-awan-tumbuh-53-4-percent>. Diakses pada 10 Oktober 2011

bahwa Indonesia sebenarnya adalah salah satu dari 20 besar dunia dalam jumlah pengguna internet – yaitu peringkat 11 - dengan hampir 40.000.000 pengguna internet pada Juni 2011[13]. Namun, penetrasi internet hanya 16 persen dari total penduduk Indonesia, dimana berarti ada ruang besar untuk pertumbuhan, meskipun tak dapat dipungkiri bahwa Indonesia masih mengalami kendala pada kurangnya infrastruktur[14].

Sistem komputasi awan kian diminati di Indonesia seiring dengan semakin banyaknya perusahaan-perusahaan besar di tanah air yang menggunakan dan tertarik untuk mengadopsi sistem mutakhir itu. Prospek pasar komputasi awan di Indonesia, masih terbuka lebar[15]. Bahkan layanan berbasis komputasi awan bakal menjadi tren ke depannya, sehingga keberadaannya tidak bisa direm. Banyak perusahaan, intansi pemerintah pusat dan daerah juga Usaha Kecil Menengah (UKM) yang memiliki storage, server, aplikasi untuk menyimpan data sangat membutuhkan *cloud computing*.[16]

Tidak ada data pasti kapan demam c*loud* itu mulai mewabah. Dalam lima tahun terakhir, pembicaraan *cloud* semakin menghangat. Riset terbaru Gartner menempatkan komputasi awandan virtualisasi di urutan dua teratas sebagai prioritas para Chief Information Officer (CIO) pada 2011 terutama untuk memacu pertumbuhan keuntungan perusahaan[17]

Springboard Research melakukan studi terhadap 114 perusahaan di Indonesia dan secara regional terhadap 833 orang CIO serta pemimpin bisnis di 8 pasar utama Asia Pasifik (APAC), pada bulan Desember 2010 sampai Maret 2011 lalu dan menemukan Komputasi Awan akan menjadi sebuah kebutuhan organisasi bisnis, pemerintah maupun nirlaba di Indonesia. Diperkirakan dalam waktu 12

[13] Top 20 Countries With The Highest Number of Internet Users, <http://www.internetworldstats.com/top20.htm> Diakses pada 20 Agustus 2011

[14] International Cloud Computing Trend : Indonesia, <http://www.cloudbusinessreview.com/2011/08/15/international-cloud-computing-trend-indonesia.html> Diakses pada 20 Agustus 2011

[15] Pasar Cloud Computing di Indonesia Terbuka Lebar. <http://www.kabarbisnis.com/read/2818810>. Diakses pada 20 Agustus 2011

[16] Ibid.

[17] Reska K. Nistanto, "Membidik UKM dengan Cloud," Bloomberg Businessweek (14-20 April 2011), hlm. 16.

hingga 18 bulan ke depan, Cloud akan mencatat pertumbuhan penting di Indonesia. Suatu studi Springboard Research mengungkap 50 persen dari organisasi di Indonesia yang ada saat ini, telah menggunakan atau dalam tahap perencanaan untuk menginisiasi penggunaan Komputasi Awan. Di antara perusahaan-perusahaan skala besar di Indonesia, animo untuk beralih kepada *cloud* saat ini meningkat hingga 68%.

Kemudian menurut hasil kajian Lembaga Pengembangan dan Pemberdayaan Masyarakat Informasi (LPPMI), industri di Indonesia cukup antusias menyikapi tren komputasi awan. Setidaknya itu yang tergambar dari hasil sampel kajian terhadap 100 perusahaan di Indonesia yang bergerak di industri teknologi informasi dan komunikasi (TIK), aktivitas profesional, sosial, serta kesehatan[18]. Dalam hasil survei yang dilakukan LPPMI disebutkan, sebanyak 62,5 persen organisasi yang ada akan menggunakan teknologi ini, meski ada juga yang berkeinginan untuk membentuk organisasi baru maupun meng-outsource implementasi *komputasi awan* pada pihak ketiga yang masing-masing presentasenya berjumlah 18,75 persen[19]

Kajian LPPMI ini juga menyebutkan ada beberapa masalah yang akan dihadapi jika responden akan menggunakan pihak ketiga dalam penyediaan komputasi awan. Namun prioritas responden untuk dimasukkan dalam kontrak kerja sama yang diantarnya adalah *Network Security Requirement* sebesar 16,66 persen, *Service Level Agreements* 15,38 persen, *Quality of Service Guarantee* (14,10 persen), dan *Auditing Activities and Certification* (14,10 persen)[20]

Kendati konsep komputasi awan sudah cukup populer, teknologi ini rupanya masih menyisakan rasa skeptis bagi perusahaan-perusahaan di wilayah ASEAN, termasuk Indonesia[21]. Belum lama ini dirilis ‘Survei Tren PC Korporat dan Perilaku Pembeli’ yang diselenggarakan oleh Lenovo bersama oleh ZDNet

[18] Indonesia Sudah Siap Sambut Komputasi Awan. <http://news.okezone.com/read/2011/05/25/324/460984/indonesia-sudah-siap-sambut-komputasi-awan.> Diakses pada 15 Agustus 2011

[19] Ibid.

[20] Ibid.

[21] Perusahaan Masih Ragu Adopsi Cloud Computing. <http://techno.okezone.com/read/2011/05/03/324/452885/perusahaan-masih-ragu-adopsi-cloud-computing>. Diakses pada 21 Agustus 2011

dan Connection Research yang dilakukan terhadap 956 pembuat keputusan teknologi informasi dari perusahaan multi nasional dan organisasi pemerintah dengan lebih dari 500 karyawan di seluruh wilayah pasar negara berkembang (ASEAN, India, Hong Kong, dan Timur Tengah & Afrika) antara bulan November dan Desember 2010. Survei tersebut juga mengungkapkan bahwa komputasi awan adalah sebuah perkembangan penting. Hampir dua-pertiga (65,6%) responden mengakui bahwa komputasi awan menjadi tren dimasa depan. Akan tetapi masih banyak yang tidak yakin dengan pendekatan yang ada saat ini dan lebih memilih untuk mengelola sendiri pemrosesan data mereka (70,2%) dan sepertiga (36,2%) masih enggan mempercayakan data mereka kepada komputasi awan[22]

Menurut laporan Goldman Sachs Equity Research pada tahun 2011, 70 persen dari CIO yang disurvei menyatakan perhatian utama mereka mengenai keamanan data di *cloud*. Perhatian mereka termasuk tidak adanya transparansi dan kontrol atas data bisnis, di mana data itu berada dan bagaimana ia dilindungi dalam infrastruktur awan yang diberikan[23]

Komputasi awan dapat membantu para pelaku bisnis untuk mengurangi biaya karena pengguna tidak perlu berinvestasi pada perangkat keras dan infrastruktur fisik lainnya, data disimpan pada lokasi yang aman dan pengguna hanya membayar untuk apa yang anda gunakan – dan tidak ada biaya lisensi yang terkait dengan komputasi awan. Tetapi terdapat beberapa permasalahan hukum yang melingkupinya seperti antara lain[24] :

1. Lokasi Fisik Data Anda

Dimana data anda disimpan secara fisik? Data Anda dapat disimpan di setiap negara dan Anda mungkin tidak tahu di mana pusat data tersebut berada. Penempatan tersebut menimbulkan pertanyaan tentang tata hukum atas data yang

[22] A Corporate PC Trends and Buyer Behaviour Survey. <http://www.lenovo.com/news/za/en/2011/03/survey.html> Diakses pada 21 Agustus 2011

[23] Pravin Kothari. Building Trust In The Cloud. <http://www.siliconindia.com/magazine_articles/Building_Trust_in_the_Cloud-UNPN806818863.html> . Diakses pada 13 September 2011

[24] The Legal Issues Around Cloud Computing. <http://www.labnol.org/internet/cloud-computing-legal-issues/14120> Diakses pada 22 Agustus 2011

disimpan itu. Konsumen harus mengetahui dengan jelas dengan ketentuan hukum yang berlaku di negara tertentu. Kemudian jika timbul sengketa, dimanakah yurisdiksi yang akan dipilih? Dalam konflik yang timbul antara penyedia layanan komputasi awan dan konsumen, sistem hukum negara mana yang akan menyelesaikan sengketa tersebut?

2. Tanggung Jawab Terhadap Data Anda.

Bagaimana jika data center terkena bencana? Adalah mungkin terjadi bahwa lokasi penyedia layanan komputasi awan adalah rentan terpengaruh karena bencana. Dalam publikasi 10-K dari Google Inc dengan *United States Securities and Exchange Commission* menyebutkan risiko seperti:

"The availability of our products and services depends on the continuing operation of our information technology and communications systems. Our systems are vulnerable to damage or interruption from earthquakes, terrorist attacks, floods, fires, power loss, telecommunications failures, computer viruses, computer denial of service attacks, or other attempts to harm our systems. Some of our data centers are located in areas with a high risk of major earthquakes. Our data centers are also subject to break-ins, sabotage, and intentional acts of vandalism, and to potential disruptions if the operators of these facilities have financial difficulties. Some of our systems are not fully redundant, and our disaster recovery planning cannot account for all eventualities. The occurrence of a natural disaster, a decision to close a facility we are using without adequate notice for financial reasons, or other unanticipated problems at our data centers could result in lengthy interruptions in our service. In addition, our products and services are highly technical and complex and may contain errors or vulnerabilities".[25]

Kemudian apakah ada cakupan kewajiban untuk pelanggaran privasi? Jika terjadi pelanggaran privasi karena kesalahan penyedia layanan awan, apakah ada cakupan kewajiban yang harus diambil atau dibayar oleh penyedia layanan kepada pengguna? Kemudian apa yang dapat dilakukan jika pusat data diretas? Meskipun semua vendor awan mencoba yang terbaik untuk melawan dan menangkis serangan hacker, tetapi jika data center dapat diretas, apakah konsumen dapat menuntut penyedia layanan untuk mengklaim adanya kehilangan keuntungan?

3. Akses dari Pihak Ketiga

[25] Annual Report Form 10-K Google Inc and United States Securities and Exchange Comission. <http://investor.google.com/documents/20101231_google_10K.html> Comission file number 000-50726. Diakses pada 27 Agustus 2011. Hlm 52

Penyedia layanan komputasi awan dapat memberikan beberapa hak istimewa kepada pihak ketiga untuk mengakses ke data Anda yang tersimpan di pusat data. Identitas pihak tersebut, jika ada, harus diungkapkan kepada pelanggan. Di sini, pihak ketiga bisa saja otoritas hukum (penyidik kepolisian dan lainnya) atau bahkan pegawai internal dari penyedia layanan. Pelanggan selalu harus diberitahu sebelum penyedia layanan memungkinkan pihak ketiga untuk mengakses data yang tersimpan.

Masih segar di ingatan kita mengenai kasus-kasus pembobolan data pelanggan yang menyerang korporasi raksasa Jepang, Sony Corp. Pada April lalu, sekelompok hacker membobol jaringan playstation Sony dan mencuri data lebih dari 77 juta account. Serangan ini dipercaya terbesar dalam sejarah Internet yang menyebabkan Sony menutup Playstation Network. Akibat pembobolan itu, perusahaan memperkirakan bakal kehilangan keuntungan hingga Rp 1,45 trilun[26]. Sebagai kompensasi Sony telah menawarkan insentif bagi pengguna PlayStation Network untuk kembali ke sistem mereka setelah terjadinya serangan hack[27]. Paket kompensasi yang diberikan oleh Sony termasuk pilihan game gratis dan tambahan hari bagi konten premium termasuk juga program 12-bulan perlindungan identitas gratis.. Inilah kekhawatiran terbesar bagi pengguna layanan komputasi awan. Data adalah harta yang tak ternilai. Di situ pulalah reputasi perusahaan dipertaruhkan.

Contoh bagaimana perlindungan data begitu penting antara lain adalah mengenai data pertahanan keamanan negara dan data pasar modal. Pada pertahanan keamanan negara, banyak informasi dan data yang bersifat rahasia yang walaupun tidak memiliki nilai komersial, tetapi apabila jatuh ke tangan orang-orang yang tidak berwenang ada kemungkinan dapat mengganggu stabilitas nasional seperti data peta wilayah, data kekuatan pasukan, dan jenis dan jumlah persenjataan. Sedangkan dalam kegiatan pasar modal, data merupakan sesuatu

[26] Jaringan Sony Dibobol Lagi, Jutaan Data Dicuri. <http://www.tempo.co/hg/it/2011/06/03/brk,20110603-338366,id.html> Diakses pada 13 September 2011

[27] "Sony offers PlayStation Network apology package",<http://www.bbc.co.uk/news/technology-13424923>, Diakses pada 13 September 2011

yang vital karena itu perlindungan data dalam pasar modal begitu sangat signifikan terkait dengan penggunaan data termasuk juga infrastukturnya[28].

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.[29]

Bagaimana mengenai regulasi di Indonesia yang mengatur mengenai Komputasi Awan? Kementerian Komunikasi dan Informatika menilai bahwa UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (LN No. 58 tahun 2008, TLN 4843) serta SNI 27000 tentang Standar Sistem Keamanan Informasi dapat menjadi regulasi acuan penerapan teknologi Komputasi Awan. Tetapi apakah regulasi yang ada sudah dapat memberikan perlindungan konsumen pengguna layanan Komputasi Awan di Indonesia?

Berdasarkan banyaknya pertanyaan hukum yang melingkupi teknologi yang terbilang baru ini, maka penulis tertarik untuk membuat penelitian dan menulis skripsi dengan judul "Analisa Yuridis Mengenai Perlindungan Data Pribadi Pada Komputasi Awan (Cloud Computing) Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik" untuk mencoba memberikan jawaban terkait jaminan hukum dan melindungi kepentingan konsumen baik personal maupun perusahaan yang menggunakan jasa fasilitas penyedia layanan Komputasi Awan terhadap data pribadi mereka di Indonesia

1.2 Pokok Permasalahan

[28] Indonesia, Undang-Undang No. 8 Tahun 1995 tentang Pasar Modal, ps. 90-99 dan 104

[29] Indonesia, Undang-Undang tentang Informasi dan Transaksi Elektronik, UU No. 11 Tahun 2008. LN No. 58 tahun 2008, TLN 4843, Penjelasan umum

Berdasarkan uraian latar belakang masalah, maka dalam penelitian ini telah dirumuskan beberapa masalah yang akan ditelaah secara ilmiah. Berikut beberapa permasalahan yang diangkat dalam penelitian ini :

1. Bagaimana perbandingan pengaturan regulasi Perlindungan Data di Uni Eropa dan Malaysia dengan Undang-Undang Informasi dan Transaksi Elektronik?
2. Bagaimana Undang-Undang Informasi dan Transaksi Elektronik melindungi data pribadi dari pengguna Komputasi Awan di Indonesia?
3. Bagaimana tanggung jawab penyedia layanan komputasi awan terhadap perlindungan data pribadi pengguna layanan komputasi awan?

1.3 Tujuan dan Manfaat Penelitian

Penelitian ini dilakukan berkaitan dengan kehendak dan maksud yang ingin dicapai, yaitu :

1.3.1 Tujuan Umum

Berdasarkan rumusan pokok permasalahan, penelitian ini memiliki tujuan umum yaitu mengumpulkan data mengenai perlindungan data pribadi di ranah hukum telematika, dalam hal ini memberikan gambaran khususnya terkait perlindungan data pribadi dalam komputasi awan. Hal ini untuk mengakomodir pesatnya perkembangan teknologi informasi dengan pengaturan pranata hukum yang terkait padanya

1.3.2. Tujuan Khusus

Tujuan khusus diadakannya penelitian ini adalah sebagai berikut :

a. Penelitian ini bertujuan untuk mengetahui perbandingan sistem perlindungan data pribadi di Uni Eropa, Malaysia dan Indonesia

b. Penelitian ini juga bertujuan untuk meninjau pengaturan Undang-undang Informasi dan Transaksi Elektronik dalam

melindngi data pribadi dari pengguna komputasi awan di Indonesia

c. Penelitian ini bertujuan untuk mengetahui tanggung jawab penyedia layanan komputasi awan terhadap perlindungan data pribadi pengguna layanan komputasi awan

.

1.4 Definisi Operasional

Dalam penulisan penelitian "Analisa Yuridis Mengenai Perlindungan Data Pribadi Dalam Komputasi Awan (Cloud Computing) Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik" ini akan cukup banyak memakai istilah dalam bidang hukum dan bidang teknologi informasi. Dan agar tidak terjadi adanya kesimpangsiuran pengertian mengenai istilah yang dipakai dalam penulisan ini, berikut dijelaskan definisi operasional dari istilah tersebut:

Komputasi Awan (Cloud Computing) adalah :

> *Cloud computing is an information-processing model in which centrally administered computing capabilities are delivered as services, on an as-needed basis, across the network to a variety of user-facing devices.*[30]

Terjemahan bebasnya adalah : Komputasi awan adalah suatu model pengolahan informasi yang dikelola terpusat memberikan kemampuan komputasi sebagai layanan yang diperlukan, melalui jaringan untuk berbagai perangkat yang digunakan oleh pengguna

Penyimpanan Awan (Cloud Storage) adalah :

[30] Chee, Brian J.S. dan Curtis Franklin, Jr., Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center. (Gainesville : CRC Press, 2010), hlm 3

> *A model of networked online storage where data is stored on multiple virtual servers, generally hosted by third parties, rather than being hosted on dedicated servers.*[31]

Terjemahan bebasnya adalah suatu bentuk penyimpanan online dalam jaringan dimana data disimpan pada beberapa server virtual, umumnya diselenggarakan oleh pihak ketiga, bukan menggunakan server sendiri.

Komputer adalah :

> Alat untuk memproses data elektronik, magnetic, optic, atau sistem yang melaksanakan fungsi logika, aritmatika dan penyimpanan[32]

Data adalah :

> Semua fakta yang dipresentasikan sebagai masukan baik dalam bentuk untaian kata (*teks*), angka (*numeric*), gambar pencitraan (*images*), suara (*voices*), ataupun gerak (*sensor*), yang telah diproses ataupun telah mengalami perubahan bentuk atau pertambahan nilai menjadi suatu bentuk yang lebih berarti sesuai dengan konteksnya

Data Pribadi (Personal Data) adalah :

> Data yang berhubungan dengan seorang individu yang hidup yang dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh*data controller*[33]

1.5 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

---

[31] Wikipedia Online Encyclopedia, "Definiton of Cloud Storage," <http://en.wikipedia.org/wiki/Cloud_storage>, diakses 11 September 2011.

[32] Indonesia, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ps. 1 butir 14

[33] Inggris, Data Protection Act 1998, Pasal 1

1. Tipe Penelitian

Penelitian ini menggunakan metode penelitian hukum yang bersifat normatif dimana data akan diperoleh dari membaca dan menganalisa bahan-bahan yang tertulis. Penelitian ini melakukan pendekatan kualitatif yang melihat dan menganalisis norma-norma hukum dalam peraturan perundang-undangan yang berkembang dalam lingkup teknologi informasi. Penelitian ini merupakan penelitian yang dilakukan secara mono-disipliner yaitu analisis terhadap temuan yang hanya didasarkan pada satu disiplin ilmu, yaitu ilmu hukum.

Alat pengumpul data yang digunakan dalam penelitian ini adalah studi dokumen dan penulis juga akan menggunakan alat pengumpul data lain selain studi dokumen, yaitu wawancara dengan narasumber[34]

Karena begitu luasnya konsep Komputasi Awan yang berkembang, maka dalam penelitian ini hanya dibatasi pada kategori Komputasi Awan yang termasuk dalam kategori *Infrastructure-as-a-Service* (IaaS)

2. Jenis Data

Penelitian ini bersifat studi kepustakaan dimana penelitian akan dilakukan dengan mengkaji informasi-informasi hukum tertulis terkait yang berasal dari berbagai sumber dan dipublikasikan secara luas serta dibutuhkan dalam penelitian normatif. Adapun data yang peneliti gunakan dalam penelitian ini terdiri dari :

a. Bahan Hukum Primer

Adalah data yang mempunyai kekuatan mengikat secara umum maupun bagi pihak-pihak yang berkepentingan. Disini data primer yang digunakan antara lain :

1. Peraturan perundang-undangan di Indonesia seperti Undang-Undang Dasar 1945, Undang-Undang No. 11 Tahun 2008 tentang

[34] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat,* ed. 1., (Jakarta : Raja Grafindo, 2006). Hal 22

Informasi dan Transaksi Elektronik, Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, dan Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik

2. Peraturan perundang-undangan di negara lain seperti United Kingdom Data Protection Act 1998, United States Privacy Act 1974 dan European Union Data Protection Directive, dan Malaysia PersonalData Protection Act 2010

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan terhadap bahan hukum primer. Bahan hukum sekunder yang akan digunakan dalam penelitian ini berupa buku, jurnal ilmiah, artikel-artikel, skripsi, tesis, makalah terkait maupun hasil pendapat orang lain yang berhubungan dengan objek penelitian.

c. Bahan Hukum Tersier

Bahan hukum tersier yang digunakan antara lain adalah kamus hukum Black's Law Dictionary

I.6 Kegunaan Teoritis dan Praktis

Penelitian yang dilakukan ini secara teoritis berguna dalam pengembangan hukum telematika terkait dengan perlindungan data pada umumnya dan secara praktis adalah untuk mendapatkan jawaban apakah pranata hukum telematika yang sudah ada di Indonesia ini sudah cukup dapat melindungi kepentingan antara konsumen yang menggunakan jasa *cloud* dari provider *cloud* serta investor yang ingin menanamkan modalnya di Indonesia pada bidang cloud ini

1.6 Sistematika Penulisan

Sistematika penulisan yang menggambarkan isi dalam penelitian ini dibagi menjadi 5 (lima) bab yaitu:

BAB 1 PENDAHULUAN

Bab ini memaparkan mengenai latar belakang masalah yang menjadi dasar penulis mengambil topik ini sebagai subjek penelitian pokok permasalahan, tujuan penelitian, definisi operasional, metode penelitian sebagai sarana untuk mencapai hasil penelitian secara metodologis dan sistematis, dan sistematika penulisan yang merupakan kerangka dari penelitian ini.

BAB 2 TINJAUAN UMUM HUKUM TELEMATIK TENTANG PERLINDUNGAN DATA

Bab Kedua merupakan bab yang berisikan tinjauan umum Hukum Telematika tentang Perlindungan Data. Dalam bab ini terbagi menjadi 3 sub-bab yang akan membahas mengenai definisi data dan perlindungan data, prinsip-prinsip perlindungan data pribadi, pengaturan perlindungan data pribadi di Indonesia sebelum dan sesudah berlakunya UU ITE, dan pengaturan perlindungan data pribadi di beberapa negara yaitu di Amerika Serikat, Inggris, Uni Eropa dan Malaysia

.

BAB 3 TINJAUAN UMUM TENTANG KOMPUTASI AWAN

Dalam bab ini akan diuraikan mengenai sekilas tentang sejarah komputasi awan berserta perkembangannya hingga saat ini, pemaparan mengenai berbagai elemen dasar layanan komputasi awan, karakteristik komputasi awan, keuntungan bisnis dari penerapan komputasi awan dan keamanan data dalam komputasi awa

BAB 4 PERLINDUNGAN DATA PRIBADI DALAM KOMPUTASI AWAN (CLOUD COMPUTING) DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Dalam bab ini menguraikan mengenai tanggung jawab penyedia layanan komputasi awan terhadap data konsumen pada beberapa kasus pembobolan data konsumen, analisis perbandingan regulasi perlindungan data di Uni Eropa dan Malaysia dengan UU ITE, analisis pasal 26 UU ITE terkait pada perlindungan data pribadi pada komputasi awan di Indonesia dan analisis perbandingan kesesuaian Terms and Condition

pada beberapa provider komputasi awan dengan prinsip-prinsip perlindungan data.

BAB 5 PENUTUP

Dalam bab ini diuraikan mengenai dua hal, yaitu kesimpulan dari hasil penelitian ini dan saran terhadap permasalahan perlindungan data pribadi dalam komputasi awan yang ditinjau dari UU Informasi dan Transaksi Elektronik.

BAB 2
TINJAUAN UMUM HUKUM TELEMATIKA TENTANG PERLINDUNGAN DATA

Dalam bab ini akan diuraikan secara khusus untuk menerangkan mengenai perlindungan data pribadi dalam hukum telematika, baik secara teori-teori dan doktrin secara umum maupun pengaturannya dalam beberapa peraturan perundang-undangan yang berlaku diluar daripada Undang-Undang Informasi dan Transaksi Elektronik. Kemudian akan diuraikan mengenai keamanan dan kerahasiaan data dalam komputer dan internet. Dan juga akan diuraikan perlindungan data di Uni Eropa, Inggris, Amerika Serikat dan Malaysia

2.1 Tinjauan Umum Tentang Perlindungan Data

Pada dewasa ini, informasi merupakan suatu media yang sangat menentukan bagi perkembangan ekonomi suatu negara baik negara berkembang maupun negara maju[35]. Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidaktelitian atau pembocoran informasi akan jauh lebih besar[36]. Era digital telah memicu ledakan pertumbuhan data pribadi yang dibuat, disimpan dan ditransmisikan pada komputer dan perangkat mobile, broadband dan situs internet dan media[37]. Kemajuan teknologi juga menimbulkan ancaman serius bagi privasi pribadi dan keamanan informasi.

Dalam konsep hukum telematika, data merupakan representasi formal suatu konsep, fakta, atau instruksi. Dalam penggunaan sehari-hari data berarti

[35] Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, (Bandung : Widya Padjajaran, 2009), hlm 53

[36] Paul Marrett, Information Law in Practice : 2nd Edition, (Cornwall : MPG Books Ltd., 2002). Hlm. 95

[37]Cameron G. Shilling, "Privacy and Data Security : New Challenges of The Digital Age", *New Hampshire Bar Journal* (2011). Hlm 1

suatu pernyataan yang diterima secara apa adanya. Data adalah bentuk jama dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan"[38].

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[39] .

Data adalah sekumpulan fakta kasar yang masih perlu di olahagar bermakna. Basisnya pada teknologi. Sedangkan Informasiadalah data yang diinterpretasikan dengan berbagai cara yangberarti, melalui prosedur dan alat bantu tertentu dengan basisnyapada pengetahuan.Menurut Davis (1985) data adalah bahan baku untuk memproduksiinformasi, sementara menurut Arnold et.al. (1972) data adalahfakta, gambar, surat, kata-kata, bagan atau simbol, yang merepresentasikanide, obyek, kondisi atau situasi.Menurut Toto (2006), Informasi adalah merupakan hasil dariproses pengolahan data yang disimpan, diproses, dan disiarkansebagai suatu pesan dalam bentuk yang lebih berguna danberarti bagi penerimanya, sehingga dapat menggambarkankejadian yang nyata dan dapat digunakan untuk pengambilankeputusan.

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[40].

Baik data maupun informasi keduanya merupakan sumberdayayang sangat penting bagi jalannya organisasi. Pada era sekarangini organisasi yang mampu menggunakan data dan informasisecara benar, cepat, tepat dan lengkap akan mampu bersaingdengan rivalnya.Pengambilan keputusan sebagai bagian dari

[38] Purwanto, Penelitian Tentang Perlindungan Hukum Data Digital, (Jakarta: Badan Pembinaan Hukum Nasional, 2007), hlm. 13

[39] Inggris, Data Protection Act 1998, Pasal 1 ayat 1

[40]Purwanto. Ibid. Hlm 14

kegiatan manusiadan selalu ada sepanjang aktivitasnya tidak terlepas dari adanyadata dan informasi ini. Tidak akan ada pengambilan keputusanmanakala tidak ada data dan informasi.

Istilah perlindungan data pertama digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur perlindungan data pribadi melalui undang-undang[41]. Alasannya dibuat perlindungan 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. Maka daripada itu agar penggunaan data pribadi tidak disalahgunakan maka diperlukan pengaturan.

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[42]. 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 membatas orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain. Menurut Jerry Kang, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karateristik masing-masing individu[43]. Pada dasarnya bentuk perlindungan terhadap data dibagi dalam dua kategori, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data

[41]Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Hlm 37

[42] Ibid. Hlm 71

[43]Jerry Kang, "Information Privacy in Cyberspace Transaction", *Stanford Law Review Vol 50*. (April 1998), Hlm 5

itu, baik data yang kasat mata maupun data yang tidak kasat mata[44]. Bentuk perlindungan data lain adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan perusakan terhadap data itu sendiri

2.2 Tinjauan Umum Tentang Privasi

Dalam sejarah perkembangannya, privasi[45] merupakan suatu konsep yang bersifat universal dan dikenal di berbagai negara baik dalam bentuk undang-undang maupun dalam bentuk aturan etika[46]. 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 *Geheimssphare* yang berarti privasi individu[47].

Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandheis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul "The Right to Privacy" atau hak untuk tidak diganggu[48]. Dalam jurnal tersebut menurut Warren dan Brandheis dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa 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 negera. Oleh karena itu hukum harus mengakui dan melindungi hak privasi tersebut .

---

[44]Purwanto, Penelitian Tentang Perlindungan Hukum Data Digital, hlm. 13

[45]Terdapat 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

[46] Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Hlm. 7

[47]Ibid.

[48]Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Hlm 10

Alasan privasi harus dilindungi yaitu[49] : Pertama, dalam membina hubungan dengan orang lain, sesorang 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 domestic 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 didserita 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.

Privasi merupakan suatu konsep yang sangat sulit untuk didefinisikan karena setiap orang akan memberi batasan yang berbeda tergantung dari sisi mana orang akan menilainya[50] . Menurut Kamus Besar Bahasa Indonesia, privasi berarti bebas, kebebasan atau keleluasaan . Sedangkan Black's Law Dictionary mendefinisikan privasi sebagai :

> *"The right to be alone; the right of a person to be free from unwarranted public. Term "right of privacy" is generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such rights prevents governmental interference in intimate personal relationship or activities, freedom of individual to make fundamental choices involving himself, his family and his relationship with others"*

Kemudian kajian perkembangan kerahasiaan pribadi pada tataran masyarakat internasional yang juga menjunjung tinggi nilai-nilai yang

[49]Ibid, Hlm 11

[50]Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Hlm 14

memberikan jaminan dan perlindungan kehormatan atas diri pribadi, sebagaimana 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."*

Secara substantive, pengaturan privasi di dalam pasal 12 UDHR ini sangat luas karena terdiri dari[51] :

1. *Physical Privacy* yaitu perlindungan privasi yang berkaitan dengan tempat tinggalnya, contohnya seseorang tidak boleh memasuki rumah orang lain tanpa izin pemilik, negara tidak boleh menggeledah rumah seseorang tanpa adanya surat penahanan, negara tidak boleh melakukan penyadapan terhadap tempat tinggal seseorang
2. *Decisional Privacy* yaitu perlindungan privasi terhadap hak untuk menentukan kehidupannya sendiri termasuk kehidupan keluarganya, contohnya dia mempunyai hak untuk menentukan kehidupan rumah tangganya sendiri.
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 Hak-Hak 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*
2. *Everyone has the right to the protection of the law against such interference or attacks*

[51]Ibid. Hlm 24

Pengaturan privasi di dalam Pasal 17 tersebut diatas menambah kata *arbitrary* atau *unlawful* atau secara melawan hukum sehubungan negara-negara tidak hanya diberi kewajiban untuk melindungi warga negaranya melalui pengaturan tetapi juga harus melarang pelanggaran privasi tersebut.[52]

Privasi sebagai suatu hak yang melekat pada setiap individu dapat dibagi menjadi beberapa jenis, yaitu[53]:

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, termasuk aparat pemerintah. Negara melalui pemerintah perlu memberikan jaminan

[52]Ibid. Hlm 25

[53] Danrivanto Budhijanto, "The Present and Future of Communication and Information Privacy in Indonesia", Jurnal Hukum Internasional Universitas Padjadjaran, Vol. 2 No. 2 (Agustus 2003), hlm. 140

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 kedalam 5 kategori yaitu[54]:

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

2.3 **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 perusakan data dan informasi perlu mendapatkan pemikiran perlindungannya[55].Keamanan dan

[54]Efrizal Fikri Yusmansyah, "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 November 2011

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

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 tingakat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan oleh kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, dimanapun, dan kapanpun mempunya kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Untuk menjaga keamanan dan kerahasiaan data dalam suatu jaringan komputer, diperlukan beberapa jenis enkripsi[56] agar data tidak dapat dibaca atau dimengerti oleh sembarangan orang kecuali untuk penerima yang berhak. Pengamanan data tersebut selain bertujuan untuk meningkatkan keamanan data, juga berfungsi untuk[57] :

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 performasi, kehandalan dan fleksibilitas software menjadi kriteria utama dan berharganya informasi tersebut dan ditunjang oleh kemampuan pengembangan

---

[56] Enkripsi 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 kasus private key cryptography) atau dengan kunci yang berbeda (untuk kasus public key cryptography).

[57] Purwanto. Ibid. Hlm 56

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 transaksi elektronik mulai diperkenalkan. Tanpa pengamanan yang ketat dan canggih, perkembangan teknologi informasi tidak memberikan manfaat yang maksimal kepada masyarakat[58].

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 lainnya[59]. Ancaman paling signfikan terhadak 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 yaitu[60] : *Intrudes*dan *Malicious Program*[61]

[58] G.A Barger, "Lost in Cyberspace : Inventors, Computer Piracy and Printed Publications under Section 102 (b) of the Patent Act of 1994", (Detroit : Mercy L. Rev), Hlm 353

[59] Purwanto. Ibid. hlm 49

[60] Ibid. hlm 50

[61]Malicious 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.

2.4 Ketentuan Hukum Perlindungan Data di Indonesia

Di Indonesia pengaturan secara khusus mengenai perlindungan data memang belum ada, namun aspek perlindungannya sudah tercermin dalam peraturan perundang-undangan lainnya[62] 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

2.4.1 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 mengetahui[63]

2.4.2 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 Perusahaan[64]. 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 terekam dalam bentuk corak apapun yang dapat dilihat, dibaca atau didengar.

---

[62]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), (Jakarta : PT. Raja Grafindo Persada, 2005), hlm 177

[63]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian),. Hlm.178

[64]Ibid.

2.4.3 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 melanggar ketentuan mengenai rahasia bank ini tentunya dengan prosedur-prosedur tertentu.[65]

2.4.4 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 penyelenggaran 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[66]. Dalam sistem kearsipan ini dapat tercakup juga data dan/atau informasi pribadi seseorang[67].

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 undang-undang 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.

[65]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Hlm 179

[66] Indonesia, Undang-Undang Tentang Kearsipan. UU No. 43 Tahun 2009. LN No. 152 Tahun 2009, TLN No. 5071, Pasal 5

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 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 pelindungan kepentingan negara dan hak-hak keperdataan rakyat melalui pengelolaan dan pemanfaatan arsip yang autentik dan terpercaya serta menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Kemudian juga disebutkan salah satu asas dalam ketentuan ini adalah asas keselamatan dan keamanan

2.4.5 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 diidentifikasikan 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 dikirimn 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 penyidik[68]

[68]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian),. Hlm. 181

2.4.6 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 berdampak terhadap perlindungan hak-hak pribadi (privacy right) seseorang[69]. 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 bersangkutan[70].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 sistim 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 harus dilakukan atas persetujuan Orang yang bersangkutan. Ayat (2) kemudian menyatakan setiap orang yang dilanggar 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:

[69] Masalah hak cipta atas hasil karya di internet mencakup berbagai jenis pelanggaran yang biasanya dilakukan oleh para Hacker, Crakcker, 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. (Jakarta : Badan Pembinaan Hukum Nasional Republik Indonesia, 2009) Hlm. 45

[70] Miller, Roger Leroy dan Jentz Gaylord, Law for E-Commerce, hlm. 233

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 luas[71]. Bagaimanapun juga, apabila ditarik penafsian 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 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 hukum[72]. 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

[71]Dionysisus Damas Pradiptya, "Pengaturan Perlindungan Data di Indonesia," *Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia*<http://indocyberlaw.org/?p=313> Diakses pada 1 November 2011

[72]Ibid.

cara apapun (manipulasi, perubahan, pernghilangan, pengrusakan) sehingga seolah-olah data tersebut menjadi data otentik[73].

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.[74]

2.4 Ketentuan Hukum Perlindungan Data Pribadi di Beberapa Negara

Hingga kini kurang lebih ada 25 negara di dunia mempunyai undang-undang mengenai perlindungan data pribadi. Sejarah mencatat bahwa negara yang mengatur pertama kali mengenai perlindungan data pribadi adalah negara bagian Hesse di Jerman, yaitu pada tahun 1970. kemudian diikuti oleh Swedia pada tahun 1973 dan Amerika Serikat pada tahun 1974 dan Inggris pada tahun 1984[75]. Dalam tulisan ini penulis ini hanya akan menggambarkan secara singkat ketentuan hukum mengenai perlindungan data pribadi yaitu yang dikeluarkan oleh Uni Eropa, Inggris, Amerika Serikat dan Malaysia

2.4.1 Uni Eropa

Pada tahun 1980, Komite Menteri-menteri dari *Organization for Economic Cooperation and Development* (OECD) mengeluarkan suatu pedoman yaitu *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Pedoman ini memberikan prinsip-prinsip dasar tentang perlindungan data dan

[73]Dionysisus Damas Pradiptya, "Pengaturan Perlindungan Data di Indonesia,"

[74]Ibid.

[75]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian),. Hlm. 164

kebebasan arus informasi (free flow of information) diantara negara-negara yang mempunyai undang-undang yang sesuai dengan prinsip-prinsip perlindungan data.

Satu tahun kemudian, Dewan Eropa (*Council of Europe*) mengumunkan suatu konvensi untuk perlindungan individu mengenai Pengolahan Data Pribadi secara otomatis (*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*) . Konvensi ini berlaku efektif para tahun 1985 yang memiliki muatan isi hampir sama dengan pedoman sebelumnya akan tetapi lebih memfokuskan pada perlindungan data untuk melindungi privasi seseorang.

Pada tanggal 20 Februari 1995 Dewan Menteri Uni Eropa menyetujui rancangan petunjuk/instruksi (Directive) yang disebut sebagai "*Directive 95/46/EC of the Parliament and The Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.*" Directive ini secara formal disetujui pada tanggal 24 Oktober 1995 dan baru akan berlaku efektif tiga tahun kemudian yaitu pada tahun 1998. Directive ini mengharuskan kelima belas negara Uni Eropa untuk mengundangkan peraturan yang berkenaan dengan pengolahan data pribadi (*processing of personal data*).[76]

Dalam pasal 1 dinyatakan bahwa tujuan dari directive ini adalah untuk melindungi hak-hak dasar dan kebebasan dari setiap orang khususnya hak atas privasi dalam kaitannya dengan pemrosesan data pribadi. Data pribadi didefinisikan sebagai setiap informasi yang berhubungan untuk mengidentifikasikan atau dapat mengidentifikasikan seseorang. Hal ini tidak hanya berupa informasi tertulis termasuk juga foto-foto, kesan audiovisual dan rekaman suara dari seseorang atau yang dapat mengidentifikasikan seseorang.

Dalam *directive* ini pengolahan (processing) didefinisikan sebagai: "setiap tindakan atau kumpulan tindakan, baik secara otomatis maupun tidak, termasuk, tetapi tidak terbatas pada pengumpulan, perekaman, pengorganisasian, penyimpanan, penyesuaian, atau perubahan, pencairan, konsultasi, penggunaan, penyingkapan, dengan pengiriman, penyebaran, atau cara lainnya yang bijak, penjajaran atau kombinasi pembatasan, penghapusan atau pengrusakan."

[76]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Hlm 166

Sehubungan dengan itu, perlu diketahui bahwa pihak-pihak yang diatur dalam directive ini adalah antara lain sebagai berikut[77]:

a. Subjek data, yaitu orang yang data pribadinya diproses.
b. *Controller*, yaitu pribadi kodrati atau pribadi hukum, otoritas publik, agen atau lembaga lain yang baik sendiri maupun bersama-sama menentukan tujuan dan cara pemrosesan data pribadi; jika tujuan dan cara pemrosesan data ditentukan oleh negara atau undang-undang, controller ditentukan oleh negara atau undang-undang.
c. *Processor*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang memproses data pribadi atas nama controller.
d. *Third party*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain kecuali subjek data, controller, processor, atau orang lain di bawah wewenang controller atau processor, berwenang untuk mengolah data.
e. *Recipient*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang kepadanya data disingkapkan.
f. *Supervisory Authorities*, yaitu badan/lembaga publik yang independen pribadi, yang mempunyai wewenang untuk menyelidiki kegiatan pengolahan data, termasuk hak untuk mengakses data tersebut dan wewenang untuk menghalangi pengiriman data ke pihak ketiga. Badan ini harus juga mendengarkan keluhan dari subjek data dan harus mengeluarkan laporan paling tidak laporan tahunan sesuai dengan undang-undang perlindungan data.yang bertugas mengawasi perlindungan data

Ruang lingkup *directive* ini diterapkan pada pemrosesan data pribadi, baik secara keseluruhan ataupun sebagian dengan alat otomatis, dan directive ini tidak dapat diterapkan pada dua hal, yaitu terhadap masalah keamanan nasional dan Undang-Undang Tindak Pidana, dan mengenai pengolahan data pribadi yang dilakukan oleh orang (pribadi kodrati) dalam kegiatan murni untuk kepentingan pribadi. Undang-undang nasional yang dibuat dalam rangka pemenuhan directive ini harus menjamin agar pemrosesan data pribadi akurat, *up to date*, relevan dan

[77]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Hlm 167

tidak berlebih-lebihan. Data pribadi hanya dapat digunakan untuk tujuan-tujuan yang sah untuk alasan data-data tersebut dikumpulkan dan disimpan dalam suatu bentuk serta tidak boleh disimpan lebih lama dari waktu yang diperlukan untuk tujuan tersebut.

Data pribadi dapat diproses hanya dengan persetujuan dari subjek data jika secara hukum dipersyaratkan, atau untuk melindungi kepentingan umum atau kepentingan yang sah dari pihak swasta (private party), kecuali jika kepentingan-kepentingan tersebut melanggar kepentingan-kepentingan subjek data. Pemrosesan data mengenai ras atau suku bangsa, pendapat-pendapat politik, agama, bujukan-bujukan filosofis atau mengenai kesehatan atau kehidupan seksual dilarang sama sekali dan dalam kebanyakan kasus dilarang tanpa persetujuan tertulis dari subjek data. Dalam pasal 6 directive ini diatur bahwa prinsip-prinsip perlindungan data adalah sebagai berikut:

a. Data pribadi harus diperoleh secara jujur dan sah
b. Data pribadi harus dkumpulkan untuk tujuan-tujuan spesifik, eksplisit dan sah serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan-tujuan tersebut. Pengolahan lebih lanjut data tersebut untuk kepentingan sejarah statistik dan ilmiah diizinkan dengan memberikan perlindungan-perlindungan.
c. Pengumpulan data harus sesuai (cukup), relevan dan tidak berlebih-lebihan, sesuai dengan tujuan pengumpulan dan pemrosesan lebih lanjut.
d. Data harus akurat dan jika perlu, harus up to date, setiap langkah yang baik harus diambil untuk menjamin bahwa data-data yang tidak akurat atau tidak lengkap berdasarkan tujuan dari pengumpulan dan pemrosesan lebih lanjutnya dihapus atau dibatasi.
e. Data tidak disimpan lebih lama dari yang diperlukan sesuai dengan tujuan pengumpulannya dan pemrosesannya

Dalam *directive* ini juga mengatur bahwa *controller* diwajibkan untuk melakukan kegiatan pengolahan data sesuai dengan undang-undang, jika tidak dapat dikenakan hukuman/sanksi dan setiap orang yang haknya dilanggar dapat diberikan ganti rugi.Eropa merupakan tempat pertama kalinya ada peraturan

mengenai privasi dan perlindungan data pribadi dalam undang-undang nasional dan sekarang menjadi yang paling komprehensif dalam memberikan perlindungan data terhadap privasi informasi di dunia. Perlindungan ini merupakan refleksi kesepakatan di antara negara-negara uni eropa bahwa privasi merupakan hak asasi yang sejajar dengan hak-hak asasi lainnya

Dari sudut pandang Uni Eropa, Amerika Serikat tidak memberikan perlindungan privasi yang memadai. Hal ini menghalangi proses transfer data antara negara-negara Eropa dan Amerika Serikat. Untuk mengatasi masalah ini, Komisi Eropa dan Departemen Perdagangan Amerika Serikat merumuskan suatu perjanjian bernama *Safe Harbor Agreement*[78]. Perjanjian *Safe Harbor* hanya berlaku untuk transfer antara Amerika Serikat dan Uni Eropa. Organisasi di luar Amerika Serikat yang memiliki bisnis operasi dalam Uni Eropa, harus bergantung pada mekanisme yang berbeda untuk mematuhi dengan *Transborder Transfer Principle* di Directive 95/46/EC. Prinsip ini mensyaratkan bahwa informasi identitas pribadi hanya dapat ditransfer ke negara-negara yang dianggap untuk memberikan keamanan yang memadai. Organisasi yang berbasis di AS dapat mematuhi dengan prinsip-prinsip perjanjian *Safe Harbor* sebagai pengganti syarat perlindungan yang memadai yang harus dipenuhi. Dalam rangka memenuhi perjanjian *Safe Harbor*, organisasi harus menerapkan *Safe Harbor Privacy Principles*, membuka kebijakan privasi mereka, harus tunduk pada Federal Trade Commission, memverifikasi kepatuhan dengan prinsipal melalui penilaian diri sendiri atau pihak ketiga dan mendaftarkan pada Departemen Perdagangan.

2.4.2 Inggris

Undang-Undang Perlindungan Data (Data Protection Act 1998) yang menggantikan *Data Protection Act* 1984 telah berlaku efektif sejak tanggal 1 Maret 2000. Undang-undang ini lahir akibat perkembangan penggunaan komputer yang semakin pesat yang menimbulkan kekhawatiran terhadap informasi tentang seseorang yang diproses tanpa sepengetahuan mereka serta tanpa adanya kemampuan untuk mengakses informasi tersebut atau memperbaikinya jika

[78]Gutwirth et al. (eds.), Computers, Privacy and Data Protection: an Element of Choice, (London : Springer Dordrecht,2011). Hlm 361

salah[79]. Undang-undang ini berusaha menjaga keseimbangan antara hak dari setiap individu dan kemampuan pihak lain untuk memperoses data mengenai mereka. Hal yang berubah dari undang-undang sebelumnya adalah bahwa undang-undang yang baru ini dapat diterapkan pada data yang diproses yang diproses secara manual, tidak hanya pada data yang diproses komputer saja, adanya kategori data sensitif, dan larangan pengiriman data ke negara lain yang tidak mempunyai perlindungan data yang cukup.

Para pihak yang diatur dalam ketentuan *Data Protection Act* 1998, adalah meliputi :

1. *The Data Protection Commisioner*

   Semua pengguna data yang menguasai data pribadi harus mendaftar pada badan ini.

2. *Data Subject*/subjek data

   Artinya setiap individu yang menjadi subjek dari data pribadi tersebut.

3. *Data Controller* (pengguna data)

   Artinya setiap orang yang menentukan tujuan dan cara mengolah data pribadi.

4. *Data Processor*

   Artinya yang dipersamakan dengan *computer bureau* (biro komputer), yaitu orang (di luar pegawai data controller) yang memproses data atas nama *data controller*

Dalam *Data Protection Act* 1998 ditemukan beberapa pengertian mengenai pengaturan perlindungan data, antara lain:

1. 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

[79]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Hlm 170

yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan (Pasal 1 ayat (1))[80]

2. Data pribadi adalah data yang berhubungan dengan seseorang individu yang hidup yang dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data controller (Pasal 1 ayat (1))[81]
3. Data sensitif adalah data pribadi yang terdiri dari informasi yang berhubungan dengan ras, etnis, dari seseorang individu, pendapat politiknya, keyakinan keagamaan, keanggotaan serikat pekerja, kesehatan fisik dan mental, kehidupan seksual, keberatan-keberatan oleh atau terhadap dirinya, proses peradilan dan hukuman akibat keberatan-keberatan tersebut.

Data Protection Act 1998 juga mengatur mengenai hak-hak subjek data, yaitu bahwa setiap individu yang menjadi subjek data sehubungan dengan data pribadi mengenai mereka yang dimiliki oleh orang/pihak lain mempunyai hak untuk mengakses informasi, mencegah pemrosesan yang dapat menyebabkan kerusakan atau keadaan yang membahayakan, hak untuk meminta kompensasi, hak untuk mengambil tindakan untuk membatasi, menghalang-halangi, menghapus atau menghancurkan data yang tidak akurat serta mempunyai hak untuk meminta commissioner untuk membuat penyelesaian terhadap tindakan-tindakan yang melanggar ketentuan-ketentuan dalam undang-undang ini. Meskipun demikian ketentuan dalam *Data Protection Act* 1998 juga memberikan pengecualian-pengecualian terhadap masalah-masalah yang terkait dengan keamanan nasional, kejahatan, perpajakan, kesehatan, pendidikan dan kerja sosial.

Terdapat perlindungan terhadap hak privasi yang dibuktikan dalam ketentuan *Data Protection Act* 1998 memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadi dan untuk mencegah beberapa jenis pengolahan data yang berlangsung[82]. Melalui permintaan tertulis

[80]Inggris. Data Protection Act 1998, Pasal 1 ayat (1)

[81]Ibid.

[82]Laurel J. Harbour, Ian D. MacDonald dan Eleni Gill, "Protection of Personal Data : The United Kingdom Perspective", Defense Counsel Journal (January 2003), Hlm 104

dan pembayaran tertentu, pengguna data harus memberitahu apakah data pribadi mereka sedang diproses dan, jika memang demikian, mereka harus diberi tahu mengenai keterangan data, tujuan data yang sedang diproses dan mereka kepada siapa data atau mungkin diungkapkan.

Ada beberapa pengecualian terhadap hak akses, termasuk juga pengecualian untuk informasi tunduk pada hak istimewa profesi hukum, pengolahan yang dilakukan untuk "khusus tujuan "(jurnalistik, sastra atau artistik) dan pencegahan kejahatan[83].

Subyek data juga memiliki beberapa pilihan terbuka bagi mereka untuk mengawasi kegiatan organisasi yang memproses data pribadi mereka[84]. *Pertama*, mereka dapat meminta pengguna data untuk tidak memproses data pribadi jika hal itu akan mengakibatkan kerusakan yang tidak beralasan dan substansial untuk subjek data atau yang lain. Hal Ini tidak berlaku di mana subjek data telah menyetujui untuk pemrosesan atau pengolahan data yang mana diperlukan untuk pelaksanaan kontrak di mana orang tersebut merupakan pihak untuk mematuhi kewajiban hukum dalam gugatan atau untuk perlindungan kepentingan vital. *Kedua,* subjek data dapat mencegah pemrosesan untuk tujuan pemasaran langsung, yang mencakup mengirim surat elektronik ke individu untuk mempromosikan produk atau jasa tertentu dan juga diarahkan ke *e-mail* account seseorang. *Ketiga,* berdasarkan Pasal 14 dari *Data Protection Act 1998*di mana pengadilan menemukan bahwa data pribadi diproses oleh pengontrol data tidak akurat, pengadilan dapat memerintahkan perbaikan, menghalangi, penghapusan atau kerusakan dari data tersebut. *Keempat,* pengguna data dapat dicegah untuk membuat keputusan tentang seorang individu dengan cara otomatis saja. *Kelima,* orang yang percaya bahwa mereka sedang terkena dampak langsung dari pengolahan data pribadi dapat meminta Komisaris untuk mengevaluasi proses untuk menentukan jika memenuhi ketentuan *Data Protection Act 1998*. Evaluasi ini dapat mengakibatkan penerbitan pemberitahuan informasi atau pemberitahuan penegakan hukum. Data subyek berhak untuk mengklaim kompensasi untuk setiap kerugian yang diderita sebagai akibat dari pelanggaran *Data Protection Act*

[83]Ibid

[84]Ibid.

1998 oleh pengontrol data dan mungkin juga mengklaim kompensasi untuk bahaya yang ditimbulkan.

2.4.3 Amerika Serikat

Berbeda dengan di Eropa, Amerika Serikat tidak mempunyai suatu undang-undang yang mengatur mengenai perlindungan data dan/atau informasi secara keseluruhan, mengenai pengumpulan, pengkomunikasian dan penggunaan semua informasi mengenai individu-individu. Selain itu, pengaturannya hanya dibatasi hanya suatu pihak tertentu, misalnya pemerintah atau industri-industri tertentu, misalnya perbankan, asuransi dan lain-lain[85] Beberapa ketentuan terkait adalah *US Privacy Act 1974* dan *Computer Matching and Privacy Act*[86] .

Ketentuan yang bernama *US Privacy Act 1974* ini menekankan pembatasan pengumpulan dan informasi pribadi oleh agen-agen pemerintah federal. Undang-undang ini tidak berlaku bagi pengumpulan data pribadi oleh lembaga-lembaga swasta. Undang-undang ini menekankan agar agen-agen pemerintah bertanggungjawab dalam mengumpulkan, memelihara, menggunakan atau menghapuskan catatan-catatan informasi yang dapat mengidentifikasikan seseorang dalam cara yang dapat menjamin bahwa perbuatan tersebut untuk tujuan yang sah dan berguna dan merupakan informasi yang baru dan akurat untuk tujuan penggunaannya, dan perlindungan yang cukup disediakan untuk penyalahgunaan informasi tersebut. Intinya undang-undang ini mencoba memberikan suatu kontrol pada setiap orang pada tingkatan tertentu terhadap penggunaan informasi mengenai mereka yang diproses oleh pemerintah federal. Jadi meskipun terdapat beberapa pengecualian, undang-undang ini pada umumnya melarang setiap agen pemerintah dari membuka catatan yang berhubungan dengan seseorang tanpa persetujuan orang tersebut.

[85]Edmon Makarim, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Hlm. 173

[86] Jean Slemmons Stratford dan Juri Stratford. Data Protection and Privacy in the United States and Europe. <*www.iassistdata.org/downloads/iqvol223stratford.pdf*> . *Diakses pada 16 Oktober 2011*

Departemen Kesehatan Amerika Serikat pada tahun 1973 mengemukakan prinsip-prinsip umum perlindungan data pribadi yang termuat dalam *Fair Information Practices* yang terdiri atas 5 prinsip dasar yaitu[87] :

1. *Notice / awareness*

   Konsumen harus diberitahu terlebih dahulu bahwa data pribadi mereka akan diakses oleh pihak kedua dan harus melalui beberapa proses seperti :

   a. Pemilik data harus diberi tahu tentang identifikasi para pihak yang akan mengoleksi informasi pribadinya (*identification of the entity collecting the data*)
   b. Pemilik data harus mendapat informasi mengenai tujuan penggunaan informasi pribadinya (*identification of the users to which data will be put*)
   c. Pemilik data harus diberi tahu pihak-pihak mana saja yang akan mengolah informasi pribadinya (*identification of any potential recipients of the data*)
   d. Peruntukan data tersebut (*the nature of the data collected and the means but which it is collected if not obvious*)
   e. Pemilikdata harus diberikan kesempatan untuk membiarkan atau menolak penyebaran informasi pribadinya (*whether the provisions of the requested data is voluntary or requires and the consequences of a refusal to provide the requested information*)
   f. Langkah-langkah yang harus diambil oleh pihak yang akan mengoleksi data untuk menjaga kerahasiaan, integritas serta keamanan informasi pribadinya (*steps taken by the data collector to ensure the confidentiality, integrity and quality of the data*)

2. *Choice / Consent*

[87]Shinta Dewi, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Hlm. 43 yang dikutip dari Department of Health, Education and Welfare, Advisory Committee's Report, 1973 hlm 50

Konsumen mempunyai hak untuk memilih apakah akan menyetujui atau tidak apabila informasi pribadinya akan diakses oleh pihak lain di dalam transaksi *online*. Proses ini cukup mudah dengan menge-klik pilihan ini dan biasanya muncul pada setiap website

3. *Access / Participation*

   Prinsip ini memberi peran aktif ke pada konsumen yaitu berhak untuk dapat mengakses informasi tentang dirinya kepada pihak manapun dan berhak untuk selalu mengkoreksi informasi pribadinya

4. *Integrity / Security*

   Data yang diakses harus tepat dan aman dan untuk menjaga ketepatan dan keamanan suatu data maka pihak kedua harus menempuh beberapa langkah seperti harus selalu melakukan pemeriksaan ulang tentang ketepatan datanya termasuk selalu menghubungi pihak pertama kemudian dari segi keamanan pihak kedua harus memiliki penguasaan secara teknik bagaimana untuk mengamankan data tesebut termasuk proses filterisasi sehingga data yang telah terkumpul tidak dapat ditembus oleh pihak yang tidak bertanggung jawab

5. *Enforcement / Redress*

   Suatu prinsip tidak dapat secara efektif diberlakukan apabila tidak ada mekanisme untuk penegakan hukum

Kemudian di bawah payung *US Privacy Act*, Kongres Amerika juga mengundangkan *Computer Matching and Protection Act of 1988*. UU ini mengubah beberapa ketentuan dalam US Privacy Act dengan menambahkan ketentuan baru yang mengatur penggunaan computer matching[88].Tetapi pada perkembangannya terdapat beberapa perubahan pengaturan privasi data setelah diundangkannya *Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001*

[88] Computer matching adalah perbandingan secara komputerisasi tentang seorang individu untuk menentukan kelayakan untuk program-program manfaat dari Federal atau untuk tujuan pemulihan pembayaran atau tunggakan hutang melalui program tersebut

(*USA Patriot Act 2001*) yang ditandatangani oleh George Walker Bush pada 26 Oktober 2001. Undang-undang ini memberikan hak kepada penegak hukum untuk mengakses data pribadi yang disimpan oleh perusahaan yang berada di Amerika Serikat terlepas dimana data itu disimpan di seluruh dunia. Undang-undang ini juga memberikan hak untuk penegak hukum untuk mencegah perusahaan-perusahaan menginformasikan kepada pemilik data bahwa mereka harus menyerahkan datanya[89] . Sebagaimana termaktub dalam Section 215 ayat (1) *USA Patriot Act*[90] :

"The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"

Terjemahan bebasnya : Direktur Biro Investigasi Federal atau orang yang ditunjuk oleh Direktur (yang peringkat harus tidak lebih rendah dari Asisten Agen Khusus Yang Bertugas) dapat membuat aplikasi untuk perintah yang memerlukan produksi dari setiap hal yang nyata (termasuk buku, catatan, dokumen, kertas dan item lainnya) untuk penyelidikan untuk melindungi terhadap terorisme internasional atau kegiatan intelijen klandestin, asalkan bahwa penyelidikan warga Amerika Serikat tidak dilakukan semata-mata atas dasar kegiatan dilindungi oleh Amandemen Pertama Konstitusi

2.4.4 Malaysia

Malaysia *Personal Data Protection Act* (PDPA) 2010 akhirnya disahkan oleh parlemen Malaysia pada awal Mei 2010. Dengan berlakunya Undang-undang ini, maka Malaysia untuk pertama kalinya memiliki Undang-undang yang

[89] EU Cloud Data Can Be Secretly Accessed by US Authorities. http://www.theregister.co.uk/2011/07/04/eu_customer_cloud_data_may_be_handed_over_by_microsoft/ Diakses pada 16 Oktober 2011

[90] Amerika Serikat, USA Patriot Act 2001, Section 215

mengatur spesifik mengenai privasi.[91] Tujuan utama dari PDPA ini adalah untuk mengatur pengolahan data pribadi oleh pengguna data dalam konteks transaksi komersial, dengan maksud menjaga kepentingan subjek data itu.[92] Hal ini dicapai dengan memastikan bahwa persetujuan dari subyek data diperoleh sebelum pengolahan data pribadi serta memberikan data dengan subjek hak untuk mengakses, benar dan juga kontrol pengolahan data pribadi mereka..

Pengesahan PDPA ini dianggap tepat pada waktunya karena pada saat ini informasi dapat ditransfer dan ditransmisikansecara transparan dan teramat mudah.[93] Mulai dari perangkat tradisional seperti email hingga jejaring sosial, informasi pribadi sangat penting dan sekarang dapat dengan mudah disebarkan. Teknologi baru dan tren pasar yang terus berubah juga berkontribusi terhadap meningkatnya peran informasi dalam ekonomi pasar global. Informasi ini, data yang sangat pribadi dari individu yang terlibat dalam transaksi komersial, telah menjadi aset berharga.

Setiap orang akan mendapat hak-hak baru seperti hak untuk diinformasikan mengenai data pribadinya serta hak untuk mengakses, mengkoreksi dan juga mengkontrol pengolahan atau penggunaan data pribadi mereka oleh pihak lain. Untuk memenuhi syarat sebagai 'data pribadi', data harus berhubungan, baik secara langsung atau tidak langsung dengan subyek data yang dapat diidentifikasi dari data.[94] 'Data pribadi' juga harus mampu direkam dan mampu diproses secara otomatis atau manual. PDPA ini juga membuat perbedaan antara 'data pribadi' dan 'data pribadi yang sensitif' yang mencakup riwayat medis, kepercayaan agama, dan pendapat politik. Pengolahan 'data pribadi yang sensitif' membutuhkan persetujuan yang eksplisit.

Beberapa lembaga penasihat, pengawas dan penegakan hukum terkait perlindungan data dipertimbangkan untuk dibentuk seperti *Personal Data*

[91] New Data Privacy Law in Malaysia.<http://www.bakermckenzie.com/RRSingaporeNewDataPrivacyLawAug10/> Diakses pada 9 Oktober 2011

[92] Ibid.

[93] Foong Cheng Leong dan Halina Jael Abu Bakar. "Personal Data Protection Act 2010," Legal Herald (Juli – September 2010), hlm. 1

[94] Malaysia. Personal Data Protection Act 2010. Section 4

Protection Commisioner, Personal Data Protection Fund, Personal Data Protection Advisory Committee dan Komite Banding juga akan dibentuk berdasarkan Undang-undang ini.

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. Dalam Undang-undang ini akan berlaku jurisdiksi dalam 3 (tiga) keadaan[95]. Pertama, dimana pengguna data didirikan di Malaysia dan pengguna data tersebut mengolah data, baik terkait atau tidak dengan proses pendirian. Kedua, saat pengolahan data dilakukan oleh setiap orang yang diperjakan atau terlibat dengan pengguna data di Malaysia. Dan ketiga, saat pengguna data tidak didirikan di Malaysia, tetapi menggunakan infrastruktur di Malaysia untuk memproses data pribadi

Dalam UU ini tedapat pengaturan pengolahan data pribadi yang termaktub dalam tujuh prinsip hukum setiap pengguna data, yaitu *General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle; dan Access Principle* dimana pengolahan data pribadi harus mematuhi prinsip-prinsip berikut:

1. *General Principle* (Prinsip Umum)[96]

   Data pribadi tidak boleh diproses tanpa persetujuan dari subjek data[97]. Namun pengguna data[98] dapat memproses data pribadi subjek data jika diperlukan untuk hal-hal sebagai berikut:

[95] Abu Bakar Munir, "The Malaysian Personal Data Protection Bill", <http://profabm.blogspot.com/2009/12/malaysian-personal-data-protection-bill.html> Diakses pada 24 Oktober 2011

[96] Malaysia. Personal Data Protection Act 2010, Section 6

[97] Subjek Data dalam UU ini berarti individu yang menjadi subyek dari data pribadi

[98] Pengguna Data dalam UU ini berarti seseorang yang baik sendiri atau bersama-sama atau dengan yang lain memperlakukan data pribadi atau memiliki kontrol atau izin pengolahan data pribadi, tetapi tidak termasuk prosesor data

a. Untuk mengetahui pelaksanaan dari perjanjian dimana salah satu atau kedua belah pihak adalah subjek data[99]
b. Untuk mengambil langkah atas permintaan subjek data dengan tujuan untuk membuat suatu perjanjian
c. Untuk memenuhi kewajiban hukum selain kewajiban yang dibebankan dalam kontrak
d. Dalam rangka melindungi kepentingan data vital[100] subjek data
e. Untuk administrasi peradilan
f. Untuk pelaksanaan fungsi-fungsi yang diberikan pada setiap orang oleh atau menurut hukum

Kemudian data pribadi tidak akan diproses kecuali:

a. Data pribadi diproses untuk maksud yang sah berhubungan secara langsung terkait dengan aktivitas pengguna data
b. Pengolahan data pribadi yang perlu bagi atau berhubungan secara langsung dengan maksud itu
c. Data pribadi yang mencukupi namun tidak berlebihan dalam kaitannya dengan maksud itu

2. *Notice and Choice Principle* (Pemberitahuan dan pilihan prinsip)[101]

Seorang pengguna data harus dengan pemberitahuan tertulis menginformasikan subjek data :

a. Bahwa data pribadi dari subjek data sedang diproses oleh atau atas nama pengguna data dan harus menyediakan deskripsi dari data pribadi tersebut kepada subjek data
b. Maksud yang pengguna data sedang atau harus dikumpulkan dan diproses lebih lanjut
c. Setiap informasi yang tersedia untuk pengguna data terkait dengan sumber data pribadi

[100] Kepentingan vital dalam Undang-undang ini berarti sesuatu yang berkaitan dengan kehidupan, kematian atau keamanan

[101] Malaysia. Personal Data Protection Act 2010, Section 7

d. Hak subjek data untuk meminta akses dan pembetulan data pribadi dan bagaimana menghubungi pengguna data dengan pertanyaan atau aduan sehubungan dengan data pribadi
e. Sekelompok pihak ketiga kepada siapa data pengguna dibuka atau dapat membuka data pribadi
f. Pilihan dan cara yang ditawarkan oleh pengguna data kepada subjek data untuk membatasi pengolahan data pribadi, termasuk data pribadi yang terkait dengan orang lain yang dapat diidentifikasi dari data pribadi itu
g. Baik wajib atau sukarela bagi subjek data untuk memberikan data pribadi
h. Dimana hal itu adalah wajib bagi subjek data untuk memberikan data pribadi, konsekuensi untuk subjek data untuk memberikan data pribadi

3. *Disclosure Principle* (Prinsip Keterbukaan)[102]

Berdasarkan Prinsip Keterbukaan, maka tidak ada data pribadi yang harus, tanpa persetujuan dari subjek data, untuk dibuka dengan tujuan apapun selain daripada:

a. Untuk tujuan dimana data pribadi harus dibuka pada saat data pribadi tersebut dikumpulkan atau tujuan yang langsung berhubungan dengan tujuan itu
b. Kepada pihak lain selain dari sekelompok dari pihak ketiga

4. *Security Principle* (Prinsip Keamanan)[103]

Seorang pengguna data wajib ketika memproses data pribadi untuk mengambil langkah-langkah praktis untuk melindungi data pribadi dari kehilangan, penyalahgunaan, modifikasi, akses yang tidak sah atau yang tidak disengaja atau terbuka, perubahan atau pengrusakan dengan memperhatikan hal-hal seperti :

[102] Malaysia. Personal Data Protection Act 2010, Section 8

[103] Ibid. Section 9

a. Sifat data pribadi dan bahaya yang akan dihasilkan dari kerugian, penyalahgunaan, modifikasi, akses yang tidak sah atau yang tidak disengaja atau terbuka, perubahan atau pengrusakan
b. Tempat atau lokasi dimana data pribadi disimpan
c. Untuk setiap langkah-langkah keamanan yang digunakan dalam peralatan apapun dimana data pribadi tersebut disimpan
d. Tindakan yang diambil untuk menjamin keandalan, integritas, dan kompetensi dari pihak yang memiliki akses ke data pribadi
e. Tindakan yang diambil untuk memastikan keamanan perpindahan data

Apabila pengolahan data pribadi dilakukan dengan data prosesor[104] atas nama pengguna data, maka pengguna data harus, untuk tujuan melindungi data pribadi dari penyalahgunaan, kehilangan, modifikasi, akses yang tidak sah atau yang tidak disengaja atau terbuka, perubahan atau pengrusakan, memastikan bahwa data prosesor :

a. Memberikan jaminan yang cukup dalam hal teknis dan langkah-langkah keamanan yang terorganisir dalam pengaturan pengolahan yang harus dilakukan
b. Mengambil langkah-langkah yang wajar untuk memastikan kepatuhan terhadap langkah-langkah tersebut

5. *Retention Principle* (Prinsip Retensi)[105]

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 semua langkah-langkah yang wajar untuk memastikan bahwa semua data pribadi dihancurkan atau dihapus secara

[104] Data Prosesor dalam Undang-undang ini adalah setiap orang, selain dari pegawai dari pengguna data, yang memproses data pribadi semata-mata atas nama pengguna data, dan tidak memproses data pribadi untuk keperluan pribadi

[105] Malaysia. Personal Data Protection Act 2010, Section 10

permanen apabila tidak lagi diperlukan untuk tujuan yang untuk itu data tersebut diproses

6. *Data Integrity Principle* (Prinsip Integritas Data)[106]

Seorang pengguna data harus mengambil langkah-langkah yang wajar untuk memastikan bahwa data pribadi yang akurat, lengkap, tidak menyesatkan dan terus diperbaharui dengan memperhatikan tujuan, termasuk secara langsung terkait dengan tujuan data pribadi tersebut dikumpulkan dan diproses lebih lanjut

7. *Access Principle* (Prinsip Akses)[107]

Subjek data harus diberikan akses ke data pribadinya yang berada pada pengguna data dan dapat melakukan perubahan data pribadinya apabila tidak akurat, tidak lengkap, menyesatkan, dan tidak sesuai, kecuali permintaan atau akses yang menurut Undang-undang ini harus ditolak.

Undang-undang ini telah menciptakan beberapa pelanggaran pidana baru untuk kegagalan dalam mematuhi ketentuan hukum. Beberapa tindak pidana yang diatur dalam Undang-undang ini antara lain : (1) bertentangan dengan prinsip Perlindungan Data Pribadi, (2) kegagalan untuk mendaftar sebagai pengguna data untuk kelas tertentu dari pengguna data, (3) pengguna data tetap meneruskan untuk memproses data pribadi setelah registrasi dicabut, (4) pengumpulan data yang melanggar hukum atau pembukaan data pribadi, (5) pengolahan data pribadi setelah penarikan persetujuan dari subyek data, (6) kegagalan untuk mematuhi persyaratan Komisaris[108]untuk menghentikan pengolahan data pribadi yang dapat menyebabkan kerusakan atau kesulitan, dan (7) kegagalan untuk mematuhi

[106]Ibid. Section 11

[107] Malaysia, Personal Data Protection Act 2010, Section 12

[108]Komisaris yang dimaksud disini adalah *Personal Data Protection Commissioner* yang bertujuan untuk menyelidiki setiap kemungkinan pelanggaran oleh pengguna data, atas keluhan dari individu atau atas inisiatif individu itu sendiri. Ketika Komisaris berpendapat bahwa pengguna data telah melanggar atau melanggar ketentuan hukum, maka Komisaris dapat melayangkan "enforcement notice"

persyaratan Komisaris untuk menghentikan pengolahan data individu untuk tujuan pemasaran langsung.

BAB 3
TINJAUAN UMUM TENTANG KOMPUTASI AWAN

Hari ini kemajuan teknologi semakin kompleks dimana teknologi telah memasuki kehidupan kita sehari-hari. Teknologi sekarang dapat harus dipahami bagi kebanyakan orang, sehingga dengan sedikit pemahaman yang lebih baik dari teknologi baru yang tersedia saat ini dapat benar-benar dapat memperkaya hidup kita.

Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. Keberadaan TIK memberikan kemudahan akses informasi menjadi lebih mudah sehingga dibalik kemudahan tersebut isu seputar cloud computing yang saat ini dikuasai oleh Google, saleforce.com, Microsoft dan Amazon.com menjadi sorotan tersendiri karena dengan perkembangan teknologi yang pesat, maka data dan informasi dapat diintegrasikan secara terpadu dan dapat diakses dimana saja dan kapan saja[109].

3.1 Sejarah Perkembangan Komputasi Awan

Saat ini komputasi awan (Cloud Computing) sudah menjadi topik hangat pembicaraan di bidang teknologi. Paling tidak kita mungkin sudah melihat banyak orang yang membahasnya melalui media massa. .Pertumbuhan pendapatan rata-rata layanan komputasi awan di Indonesia diperkirakan sebesar 48% per tahun hingga 2014.

Segmen layanan *infrastructure as a service* atau *data center* akan tumbuh paling pesat di antara layanan komputasi awan lain dengan pertumbuhan 55,9%, demikian hasil riset lembaga Frost & Sullivan[110]. Pada 7 Maret 2011, IBM mengumumkan investasi 38 miliar dollar AS (sekitar Rp 380 triliun) untuk membangun pusat data yang dinamai *IBM Asia Pacific Cloud Computing Data*

[109]Cahyana Ahmadjayadi, Pointers Kepala Badan Litbang SDM Kementerian Komunikasi dan Informatika Republik Indonesia Pada Acara Seminar Innovation Cloud Computing, Bandung, 18 Oktober 2010.

[110]Pendapatan Cloud Computing di Indonesia Tumbuh 48% hingga 2014, <http://www.indonesiafinancetoday.com/read/16131/Pendapatan-Cloud-Computing-di-Indonesia-Tumbuh-48-hingga-2014> Diakses pada 16 November 2011

*Centr*e di Singapura. Fujitsu menyusul dengan investasi 1,1 miliar dollar AS, sekaligus melakukan pelatihan kepada 5.000 spesialis teknologi komputasi awan hingga akhir 2012. Tujuannya, mengembangkan infrastruktur komputasi awan Fujitsu "*Infastructure as a Service*"[111].

Para peneliti di bidang ini mengatakan bahwa komputasi awan adalah pilihan logis untuk perkembangan komputer online di masa depan[112]. Meskipun sulit untuk memprediksi masa depan, komputasi awan telah dikembangkan oleh proyek infrastruktur di *Laboratorium Nasional Argonne*, bernama Nimbus, yang menunjukkan bahwa potensi komputasi awan sudah mulai direalisasikan sekarang. Proyek ini lah yang akan menjadi cikal bakal era komputasi awan[113] .

Komputasi awan beberapa tahun terakhir ini telah menjadi *buzzword* terpanas di dunia teknologi informasi (TI). Seluruh nama besar seperti IBM, Microsoft, Google, dan Apple, saat ini sedang terlibat dalam peperangan untuk menjadi penguasa terbesar terhadap awan ini[114]. Tentu saja masing-masing mengeluarkan produk andalannya masing-masing.

IBM di paruh akhir tahun 2009 kemarin telah meluncurkan LotusLive[115] , layanan kolaborasi berbasis *cloud*. Microsoft, yang sekarang di perkuat oleh Ray Ozzie sebagai Chief Software Architect pengganti Bill Gates, menggadang Windows Azure[116], sistem operasi berbasis *cloud* yang akan menjadi masa depan

[111]Komputasi Awan Masih Di Awang-Awang. <http://tekno.kompas.com/read/2011/07/04/03225759/Komputasi.Awan.Masih.di.Awang-awang> Diakses pada 30 November 2011

[112]Era Komputasi Awan <http://www.bunyu-online.com/2009/05/era-komputasi-awan.html> Diakses pada 14 November 2011

[113] Ibid.

[114]Mochamad James Falahuddin, "Lebih Jauh Mengenal Komputasi Awan" <http://www.detikinet.com/read/2010/02/24/084138/1305595/328/lebih-jauh-mengenal-komputasi-awan> Diakses pada 14 November 2011

[115] LotusLive adalah perpaduan layanan bisnis berbasis komputasi awan yang dijalankan oleh divisi Lotus Software IBM. Layanan terpadu dari LotusLive meliputi jaringan sosial, pertemuan bisnis online, berbagi data, instant message, visualisasi data dan email. Dapat diakses pada alamat https://www.**lotuslive**.com/

[116]Windows Azure adalah sebuah platform Microsoft yang digunakan untuk membangun dan meng-hosting web melalui Microsoft Data Centers. Platform Windows Azure diklasifikasikan sebagai "platform-as-a-service" dan menjadi bagian dari layanan komputasi awan Microsoft bersama software-as-a-service dari Microsoft yaitu Microsoft Online Services. Dapat diakses pada alamat http://www.microsoft.com/windowsazure/

Windows OS[117] . Dan competitor terbesar Windows, Apple mengambil sisi lain, telah menyediakan layanan MobileMe yang memungkinkan pengguna produk Mac, untuk melakukan sinkronisasi data ke dalam *cloud* dan pada perkembangannya Apple sendiri merestrukturisasi MobileMe dan membuat komputasi awannya sendiri dengan meluncurkan layanan iCloud[118] .

Sementara Google, satu-satunya raksasa yang lahir di era internet, sudah sejak lama memberikan layanan *Google Docs*[119] yang memungkinkan pengguna membuat dokumen atau bekerja dengan spreadsheet secara *online* tanpa memerlukan software yang terinstal di *PC* atau *notebook*. Bahkan Google dalam waktu dekat akan meluncurkan sistem operasi *cloud*-nya, Chrome OS, yang akan menjadi ancaman serius bagi para penyedia sistem operasi lain. Namun bisa dibilang, keberhasilan Salesforce.com-lah yang membuka mata dunia bahwa cloud computing menjanjikan pundi-pundi emas yang menggiurkan .

Komputasi awan seakan membangkitkan persepsi yang berbeda di tiap-tiap orang. Pada sebagai orang, komputasi awan mengacu pada suatu cara mengakses perangkat lunak dan menyimpan data dalam "awan" yang merupakan representasi dari internet atau jaringan dan menggunakan layanan-layanan yang terkait komputasi awan. Bagi pihak lain yang menganggap komputasi awan adalah sesuatu hal yang baru, tetapi bagi sebagian pihak komputasi awan hanya modernisasi dari model sejenis yang banyak digunakan pada 1960-an sebelum munculnya *platform* komputasi yang relatif lebih murah[120] .

---

[117]Mochamad James Falahuddin. Ibid.

[118] iCloud adalah layanan penyimpanan awan (cloud storage) dari Apple Inc yang diluncurkan pada tanggal 6 Juni 2011 di Apple Worldwide Developers Conference (WWDC). Layanan ini memungkinkan pengguna untuk menyimpan data seperti file musik pada server remote Apple untuk men-download untuk beberapa perangkat seperti iPhone, iPod, iPad dan komputer pribadi yang menjalankan Mac OS X atau Microsoft Windows. Program ini juga menggantikan Apple MobileMe yang sebelumnya bertindak sebagai hub untuk email, kontak, kalender, bookmark, catatan, daftar sinkronisasi data lainnya. Dapat diakses pada www.**apple**.com/**icloud**/

[119] Google Docs adalah layanan host dari Google di mana Anda dapat membuat, menyimpan dan berbagi dokumen, spreadsheet, dan presentasi, dan formulir online Anda dapat bekerja sendiri atau bersama-sama. Dapat diakses pada https://**docs**.**google**.com/

[120]Ronald L. Krutz dan Russel Dean Vines, Cloud Security : A Comprehensive Guide to Secure Cloud Computing, (Indianapolis : Wiley Publishing Inc, 2010) Hlm. 1

Sejarah komputasi awan sebagai sebuah konsep yang membawa sumber daya komputasi ke suatu posisi yang berbeda melalui jaringan global dapat dikatakan telah mulai diperkenalkan pada tahun enam puluhan oleh Joseph Carl Robnett Licklider sering disingkat JCR Licklider[121]. Ide JCR Licklider dari sebuah "jaringan komputer intergalaksi" tampaknya cukup sesuai dengan apa yang kita saat ini menyebutnya dengan komputasi awan. Licklider adalah orang yang juga bertanggung jawab dalam pengembangan ARPANET[122]. Pelopor komputasi awan adalah John McCarthy yang membayangkan pada awal 1960-an bahwa perhitungan suatu hari nanti dapat diatur sebagai utilitas publik seperti air dan listrik[123]

Namun baru di tahun 1995 lah, Larry Ellison, pendiri Oracle , memunculkan ide "Network Computing" sebagai kampanye untuk menggugat dominasi Microsoft yang saat itu merajai *desktop computing* dengan Windows 95-nya[124]. Larry Ellison menawarkan ide bahwa sebetulnya user tidak memerlukan berbagai software, mulai dari Sistem Operasi dan berbagai software lain, dijejalkan ke dalam PC Desktop mereka. PC Desktop bisa digantikan oleh sebuah terminal yang langsung terhubung dengan sebuah server yang menyediakan fasilitas-fasilitas yang berisi berbagai kebutuhan software yang siap diakses oleh pengguna. Ide "*Network Computing*" ini sempat menghangat dengan munculnya beberapa pabrikan seperti Sun Microsystem dan Novell Netware yang menawarkan *Network Computing Client* sebagai pengganti *desktop*. Namun akhirnya, gaung *Network Computing* ini lenyap dengan sendirinya, terutama

[121]Joseph Carl Robnett Licklider (11 Maret 1915 - 26 Juni 1990), yang dikenal hanya sebagai JCR atau "Lick" adalah seorang ilmuwan komputer Amerika, dianggap sebagai salah satu tokoh yang paling penting dalam ilmu komputer dan sejarah komputasi umum. Dia dikenal karena menjadi salah satu yang pertama untuk membangun komputasi interaktif modern, dan aplikasi untuk segala macam kegiatan, dan juga sebagai pelopor internet, dengan visi awal dari sebuah jaringan komputer yang terhubung di seluruh dunia jauh sebelum internet ditemukan .

[122] The Advanced Research Projects Agency Network (ARPANET) adalah packet switching network yang pertama kali dioperasikan di dunia. Jaringan ini didanai oleh Defense Advanced Research Projects Agency (DARPA) dari Departemen Pertahanan Amerika Serikat untuk digunakan oleh proyek-proyek di universitas dan laboratorium penelitian di Amerika Serikat.

[123]Cloud Computing, <http://www.syntheticlepathy.net/information-and-communication-technology/cloud-computing/> Diakses pada 14 November 2011

[124]Mochamad James Falahuddin. Ibid.

disebabkan kualitas jaringan komputer yang saat itu masih belum memadai, sehingga akses *Network Computing* ini menjadi sangat lambat, sehingga orang-orang akhirnya kembali memilih kenyamanan PC Desktop, seiring dengan semakin murahnya harga PC.

Tonggak selanjutnya adalah kehadiran konsep ASP (*Application Service Provider*) di akhir era 90-an[125]. Seiring dengan semakin meningkatnya kualitas jaringan komputer, memungkinkan akses aplikasi menjadi lebih cepat. Hal ini ditangkap sebagai peluang oleh sejumlah pemilik data center untuk menawarkan fasilitasnya sebagai tempat 'hosting' aplikasi yang dapat diakses oleh pelanggan melalui jaringan komputer. Dengan demikian pelanggan tidak perlu investasi di perangkat data center. Hanya saja ASP ini masih bersifat "privat", di mana layanan hanya dikustomisasi khusus untuk satu pelanggan tertentu, sementara aplikasi yang di sediakan waktu itu umumnya masih bersifat *client-server*.

Kehadiran berbagai teknik baru dalam pengembangan perangkat lunak di awal abad 21, terutama di area pemrograman berbasis web disertai peningkatan kapasitas jaringan internet, telah menjadikan situs-situs internet bukan lagi berisi sekedar informasi statik. Tapi sudah mulai mengarah ke aplikasi bisnis yang lebih kompleks[126].

Popularitas *Cloud Computing* semakin menjulang saat di awal 2000-an, Marc Benioff yang merupakan *ex-Vice President* di Oracle, meluncurkan layanan aplikasi CRM (*Customer Relationship Management*) dalam bentuk *Software as a Service*, Salesforce.com, yang mendapatkan sambutan gegap gempita. Dengan misinya yang terkenal yaitu "*The End of Software*", Benioff bisa dikatakan berhasil mewujudkan visi Larry Elisson tentang Network Computing menjadi kenyataan satu dekade kemudian.

Selanjutnya jargon Cloud Computing bergulir seperti bola salju menyapu dunia teknologi informasi. Dimulai di tahun 2005, mulai muncul inisiatif yang didorong oleh nama-nama besar seperti Amazon.com yang meluncurkan Amazon EC2 (*Elastic Compute Cloud*), Google dengan Google App Engine-nya, tak

[125] Ibid.

[126] Ibid.

ketinggalan raksasa biru IBM meluncurkan *Blue Cloud Initiative* dan lain sebagainya.

Semua inisiatif ini masih terus bergerak, dan bentuk *Cloud Computing* pun masih terus mencari bentuk terbaiknya, baik dari sisi praktis maupun dari sisi akademis. Bahkan dari sisi akademis, jurnal-jurnal yang membahas tentang ini hal ini baru bermunculan di tiga tahun belakangan. Akhirnya seperti yang kita saksikan sekarang, seluruh nama-nama besar terlibat dalam pertarungan menguasai awan ini. Bahkan pabrikan Dell, pernah mencoba mempatenkan istilah *"Cloud Computing*", namun ditolak oleh otoritas paten Amerika.

Walaupun di luaran perebutan kapling awan ini begitu ingar-bingar, tidak demikian dengan di tanah air Indonesia tercinta ini. Pemain yang benar-benar mencoba masuk di area ini masih sangat sedikit, bahkan jumlahnya bisa dibilang belum sebanyak jari sebelah tangan.

Salah satu yang cukup serius bermain di area ini adalah PT Telkom, yang setidaknya saat ini sudah menawarkan dua layanan aplikasi berbasis *Software as a Service*. Salah satunya melalui anak usahanya, Sigma Cipta Caraka, yang menawarkan layanan aplikasi *core banking* bagi bank kecil-menengah. Kemudian bekerjasama dengan IBM Indonesia dan mitra bisnisnya, PT Codephile, Telkom menawarkan layanan *e-Office on Demand* untuk kebutuhan kolaborasi/korespondensi di dalam suatu perusahaan atau organisasi

3.2Definisi Komputasi Awan

Dalam dunia teknologi informasi para ahli telah banyak memberikan definisi atau pengertian tentang komputasi awan antara lain :

> *Cloud computing can be defined as simply the sharing and use of applications and resources of a network environment to get work done without concern about ownership and management of the network's resources and applications. With cloud computing, computer resources for getting work done and their data are no longer stored on one's personal computer, but are hosted elsewhere to be made accessible in any location and at any time* (Scale, 2009).

> *Cloud computing is an information-processing model in whichcentrally administered computing capabilities are delivered asservices, on an as-*

needed basis, across the network to a varietyof user-facing devices(Hewitt, 2008)[127].

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization (Vaquero, 2009)[128]

Kemudian beberapa definisi komputasi awanyang dapat membantu kita untuk mengenal apa itu komputasi awan[129]:

a. Komputasi awanadalah gabungan pemanfaatan teknologi komputer ('komputasi') dan pengembangan berbasis Internet ('awan'). Awan (cloud) adalah metefora dari internet, sebagaimana awan yang sering digambarkan di diagram jaringan komputer, awan (cloud) dalam Cloud Computing juga merupakan abstraksi dari infrastruktur kompleks yang disembunyikannya.Internet Cloud adalah suatu model komputasi di mana kapabilitas terkait teknologi informasi disajikan sebagai suatu layanan, sehingga pengguna dapat mengaksesnya lewat Internet.
b. Komputasi awanadalah suatu konsep umum yang mencakup SaaS(*software as a service*), Web 2.0, dan tren teknologi terbaru lain yang dikenal luas, dengan tema umum berupa ketergantungan terhadap Internet untuk memberikan kebutuhan komputasi pengguna.
c. Komputasi awanadalah istilah untuk kegiatan menyelesaikan suatu proses atau perhitungan melalui internet dengan memanfaatkan sumber daya yang dimiliki oleh suatu kumpulan komputer yang saling terhubung di suatu tempat.
d. Komputasi awanadalah teknologi yang menggunakan internet dan server pusat yang jauh untuk menjaga/mengelola data dan aplikasi.

---

[127] Chee, Brian J.S. dan Curtis Franklin, Jr., Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center. (Gainesville : CRC Press, 2010), hlm 3

[128]Serge Gurtwith, ed, Computer, Privacy and Data Protection : an Element of Choice. (London : Springer Dordrecht), hlm. 362

[129]Herwin Anggeriana, dkk, Cloud Computing <http://lutung.lib.ums.ac.id/dokumen/ebooks/Komputer/Cloud%20Computing/Cloud-Computing.pdf> Diakses pada 5 Desember 2011 , hlm. 4-5

e. Komputasi awansecara sederhana dapat didefinisikan adalah "layanan teknologi informasi yang bisa dimanfaatkan atau diakses oleh pelanggannya melalui jaringan internet". Kata-kata "*Cloud*" sendiri merujuk kepada simbol awan yang di dunia TI digunakan untuk menggambarkan jaringan internet (internet cloud).

f. Komputasi awanbisa diartikan sebagai suatu model yang memungkinkan jaringan dapat diakses dengan mudah sesuai kebutuhan di berbagai lokasi.dimana model ini memungkinkan untuk mengumpulkan sumber daya komputasi seperti network, server, storage, aplikasi dan services dalam satu wadah.

Kehadiran komputasi awan awalnya memang hadir bagi kalangan industri. Sebagaimana yang dikatakan oleh Hartig (2008) *Cloud computing is a new model of computing that is widely being utilized in today's industry and society*. Ada beberapa alasan yang melatarbelakangi penerapan teknologi ini, antara lain :

1. Ini adalah sebuah model layanan berbasis Internet untuk menampung sumberdaya sebuah perusahaan. Artinya sebuah perusahaan tak perlu lagi memiliki atau mendirikan infrastruktur lantaran sudah ada perusahaan lain yang menyediakan “penampung” di cloud alias Internet.
2. Sebuah perusahaan tak perlu lagi mengalokasikan anggaran untuk pembelian dan perawatan infrastruktur dan software.
3. Perusahaan pun tak perlu memiliki pengetahuan serta merekrut tenaga pakar dan tenaga pengontrol infrastruktur di “cloud” yang mendukung mereka.

National Institute of Standards and Technology (NIST), *Information Technology Laboratory* memberikan dua buah catatan mengenai pengertian komputasi awan. Pertama, komputasi awan masih merupakan paradigma yang berkembang . Definisi, kasus penggunaan, teknologi yang mendasari, masalah, risiko, dan manfaat akan terus disempurnakan melalui perdebatan baik oleh sektor public maupun swasta. Definisi, atribut, dan karakteristik akan berkembang dan berubah dari waktu ke waktu. Kedua, industri komputasi awan merupakan ekosistem besar dengan banyak model, vendor, dan pangsa pasar. Definisi ini mencoba untuk mencakup semua pendekatan berbagai awan .

Dari kedua catatan tersebut NIST memberikan definisi komputasi awan adalah model untuk memungkinkan kenyaman, *on-demand* akses jaringan untuk memanfaatkan bersama suatu sumberdaya komputasi yang terkonfigurasi (misalnya, jaringan, server, penyimpanan, aplikasi, dan layanan) yang dapat secara cepat diberikan dan dirilis dengan upaya manajemen yang minimal atau interaksi penyedia layanan. Model komputasi awan mendorong ketersediaan dan terdiri dari lima karakteristik, tiga model layanan, dan empat model penyebaran

3.3Karakteristik Komputasi Awan

NIST mengidentifikasi lima karakteristik penting dari komputasi awan sebagai berikut[130] :

1. *On-demandself-service.*

   Sebuah layanan komputasi awanharus dapat dimanfaatkan oleh pengguna melalui mekanisme swalayan dan langsung tersedia pada saat dibutuhkan. Konsumen dapat menentukan sendiri kemampuan komputasi yang diinginkan, seperti waktu penggunaan server dan penyimpanan pada jaringan, tanpa harus berinteraksi langsung (antar manusia) dengan pemberi jasa layanan.

2. *Broad Network Access*

   Sebuah layanan komputasi awanharus dapat diakses dari mana saja, kapan saja, dengan alat apa pun, asalkan kita terhubung ke jaringan layanan. Kemampuan tersebut tersedia pada jaringan dan diakses melalui mekanisme standar yang dapat digunakan dengan semua jenis platform klien, *thin or thick* (misalnya, ponsel, tablet, laptop, maupun *workstation*).

3. *Resource Pooling*

   Sebuah layanan komputasi awanharus tersedia secara terpusat dan dapat membagi sumber daya secara efisien. Karena *cloud computing* digunakan bersama-sama oleh berbagai pelanggan, penyedia layanan harus dapat membagi beban secara efisien, sehingga sistem dapat dimanfaatkan secara maksimal.

[130]Ibid. Hlm. 2

4. *Rapid Elasticity*

   Kemampuan dapat secara elastis ditentukan dan diluncurkan, dalam beberapa kasus secara otomatis, pada skala yang cepat berkembang, naik maupun turun, sepadan dengan permintaan. Untuk konsumen, kemampuan yang tersedia untuk provisioning menjadi tidak terbatas dan dapat disesuaikan dalam secara kuantitas setiap saat.

5. *Measured Service*

   Sistem *cloud* secara otomatis mengontrol dan mengoptimalisasi penggunaan sumber daya, memanfaatkan kemampuan pengukuran (biasanya secara *pay-per-use* atau *charge-per-use*) pada tiap tingkat abstraksi yang sesuai dengan jenis layanan (misalnya: penyimpanan, pemrosesan, *bandwidth*, dan akun pengguna aktif). Penggunaan sumber daya dapat dipantau, dikendalikan dan dilaporkan, menciptakan keterbukaan kepada baik penyedia jasa maupun pengguna pada layanan yang dilakukan

3.4 Jenis dan Model Layanan Komputasi Awan

Terdapat tiga jenis layanan yang dijelaskan oleh NIST yaitu antara lain[131] :

1. *Software as a Service* (SaaS).

   Sebagai konsumen individual, kita sebenarnya sudah akrab dengan layanan komputasi awan melalui *Yahoo Mail*, *Hotmail*, *Google Search*, *Bing*, atau *MSN Messenger*. Contoh lain yang cukup populer adalah *Google Docs* ataupun *Microsoft Office Web Applications* yang merupakan aplikasi pengolah dokumen berbasis internet. Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur awan. Aplikasi dapat diakses dari berbagai perangkat klien melalui antarmuka seperti *web* browser (misalnya, email berbasis web). Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan

[131]Peter Mell dan Timothy Grance, "The NIST Definition of Cloud Computing," Hlm. 2-3

pengecualian terbatas terhadap pengaturan konfigurasi aplikasi pengguna tertentu.

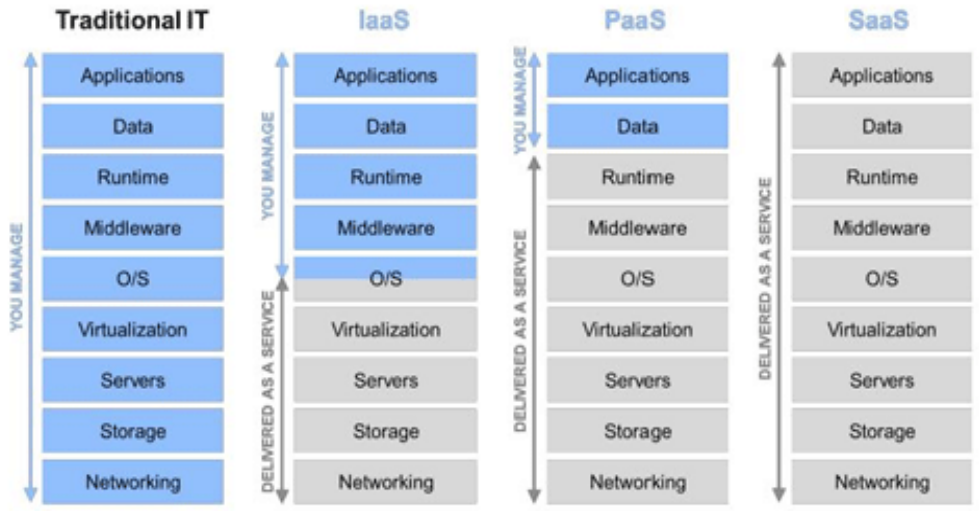
2. *Platform as a Service* (PaaS).

   Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur komputasi awan menggunakan bahasa pemrograman dan peralatan yang didukung oleh provider. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, atau penyimpanan, namun memiliki kontrol atas aplikasi disebarkan dan memungkinkan aplikasi melakukan hosting konfigurasi. Pada PaaS, kita membuat sendiri aplikasi software yang kita inginkan, termasuk skema *database* yang diperlukan. Skema itu kemudian kita pasang (*deploy)* di *server-server* milik penyedia jada PaaS. Penyedia jasa PaaS sendiri menyediakan layanan berupa platform, mulai dari mengatur server-server mereka secara virtualisasi sehingga sudah menjadi cluster sampai menyediakan sistem operasi di atasnya. Alhasil, kita sebagai pengguna hanya perlu memasang aplikasi yang kita buat di atasnya. contoh vendor penyedia layanan Paas adalah *Microsoft Azure* dan *Amazon Web Services*.

3. *Infrastructure as a Service* (IaaS).

   Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan komputasi sumberdaya lain yang penting, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas , dapat mencakup sistem operasi dan aplikasi. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari tetapi memiliki kontrol atas sistem operasi, penyimpanan, aplikasi yang disebarkan, dan mungkin kontrol terbatas komponen jaringan yang pilih (misalnya, firewall host). Pada IaaS, penyedia layanan hanya menyediakan sumber daya komputasi seperti prosesor, memori, dan storage yang sudah tervirtualisasi. Akan tetapi, penyedia layanan tidak memasang sistem operasi maupun aplikasi di atasnya. Pemilihan sistem operasi, aplikasi, maupun konfigurasi lainnya sepenuhnya berada pada kendali kita.

Perbandingan level antara penyedia dengan pengguna layanan Cloud



Source: Microsoft.

Kemudian terdapat empat model infrastruktur komputasi awan yang ada saat ini yaitu[132] :

1. *Private cloud*

   Infrastruktur awan yang semata-mata dioperasikan untuk sebuah organisasi atau perusahaan. Pengelolaannya dilakukan oleh pengguna komputasi awan itu sendiri atau menggunakan pihak ketiga yang hanya menyediakan bagi kepentingan satu organisasi/perusahaan.

2. *Community cloud.*

   Dalam model ini, sebuah infrastruktur cloud digunakan bersama-sama oleh beberapa organisasi yang memiliki kesamaan kepentingan, misalnya dari sisi misinya, atau tingkat keamanan yang dibutuhkan, dan lainnya. Jadi, *community cloud* ini merupakan "pengembangan terbatas" dari private cloud. Dan sama juga dengan private cloud, infrastruktur cloud yang ada bisa di-manage oleh salah satu dari organisasi itu, ataupun juga oleh pihak ketiga.

3. *Public cloud.*

[132]W. Michael Ryan dan Christopher M. Leoffler, "Insights into Cloud Computing" (Intellectual Property and Technology Law Journal Vol 22 Number 11 , November 2010) Hlm. 1

Seperti *Amazon Cloud* atau *Google* yang meluncurkan *Google Docs* yang tersedia untuk setiap orang atau kelompok industry yang besar dan keduanya dikelola oleh penyedia layanan komputasi awan. Model penyebaran secara public menawarkan potensi fleksibilitas dan penghematan yang sangat tinggi. Dan juga menuntut penyedia layanan untuk menyediakan kontrol yang besar atas kemampuan teknologi di perusahaan yang menggunakan jasa layanan public cloud tersebut.

4. *Hybrid cloud.*

   Untuk jenis ini, infrastruktur *cloud* yang tersedia merupakan komposisi dari dua atau lebih infrastruktur cloud (*private*, *community*, atau *public*). Di mana meskipun secara entitas mereka tetap berdiri sendiri-sendiri, tapi dihubungkan oleh suatu teknologi/mekanisme yang memungkinkan portabilitas data dan aplikasi antar *cloud* itu. Misalnya, mekanisme load balancing yang antarcloud, sehingga alokasi sumberdaya bisa dipertahankan pada level yang optimal

3.5 Keuntungan Bisnis dari Komputasi Awan

Janji penghematan keuangan merupakan insentif yang sangat menarik dimana migrasi ke komputasi awan adalah kesempatan terbaik bagi perusahaan untuk merampingkan proses dan meningkatkan inovasi. Hal ini memungkinkan peningkatan produktivitas dan mengubah proses bisnis dengan cara yang mahal sebelum penerapan komputasi awan. Perusahaan dapat fokus pada bisnis inti mereka, daripada khawatir tentang skalibilitas dan infrastruktur. Memenuhi tuntutan kinerja puncak bisnis dapat dicapai dengan mudah dengan menggunakan komputasi awan.

Meskipun ambiguitas mengelilingi pengaplikasian komputasi awan, studi kasus menunjukkan bahwa pengaplikasian komputasi awan dapat menghemat 25 sampai 50 persen dari biaya teknologi informasi di organisasi mereka[133]. Menurut makalah yang ditulis oleh Darrell M. West, Wakil Presiden dan Direktur Studi

[133]Cloud Computing for Business Cuts Cost by 50 Percent, <http://www.cloudbusinessreview.com/2010/11/20/cloud-computing-for-business-cuts-costs-by-50-percent.html> Diakses pada 30 November 2011

Pemerintahan di *Brookings Institution*, menerapkan komputasi awan dengan cara yang tepat dapat menghemat uang secara signifikan.

Makalah yang berjudul "*Saving Money Through Cloud Computing*"[134] menunjukkan beberapa studi kasus yang menarik - di sini adalah beberapa di antaranya:

1. Kota Miami menggunakan Microsoft Windows Azure sebagai pilihan dari platform awan pada tahun 2009. **Menghemat : 75 persen.**
2. Kota Los Angeles memindah layanan e-mail mereka pada tahun 2009 ke Google Cloud. **Menghemat : 23,6 persen.**
3. Pada tahun 2008, Washington, DC pemerintah kota bermigrasi e-mail nya layanan di 86 instansi ke komputasi awan. **Menghemat : 48 persen.**
4. *Cloud computing* membantu *National Aeronautics and Space Administration* (NASA) untuk mengakses sumber daya pada permintaan skala atas atau bawah sesuai dengan kebutuhan ilmiah dan kepentingan publik.

Kemudian *Information Systems Audit and Control Association* (ISACA) juga menjelaskan beberapa manfaat bisnis utama yang ditawarkan oleh komputasi awan yaitu[135] :

1. Pengendalian biaya

   Komputasi awan menawarkan pelaku bisnis pilihan skalabilitas tanpa suatu komitmen keuangan yang serius untuk pembelian dan pemeliharaan infrastruktur. Ada sedikit atau tidak ada pengeluaran modal dimuka dengan layanan berbasis awan. Penyimpanan dan layanan yang tersedia berdasarkan permintaan dan biaya sebagai layanan *pay-as-you-go*. Selain itu, komputasi awan dapat membantu dengan penghematan biaya dalam hal sumber daya seperti menghemat

[134]Makalah Darrel M. West berjudul Saving Money Through Cloud Computing dapat diunduh di : http://www.brookings.edu/~/media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf

[135]ISACA, "Cloud Computing : Business Benefits With Security, Governance and Assurance Perspective" <http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_%26_Governance-ISACA.pdf> Diakses pada 18 November 2011

ruang server yang tidak terpakai memungkinkan perusahaan untuk mengendalikan biaya dalam hal persyaratan teknologi yang ada dan bereksperimen dengan teknologi baru dan jasa tanpa investasi yang besar.

2. Kedekatan

   Banyak pengadopsi awal komputasi awan telah membuktikan kemampuan untuk penyediaan dan penggunaan layanan dalam satu hari. Dibandingkan dengan proyek-proyek teknologi informasi konvensional yang mungkin memerlukan beberapa minggu atau bulan untuk memesan, mengkonfigurasi dan mengoperasikan sumber daya yang diperlukan. Hal ini memiliki dampak yang mendasar pada kecepatan bisnis dan mengurangi biaya yang terkait dengan penundaan waktu.

3. Ketersediaan

   Penyedia layanan awan memiliki infrastruktur dan kesiapan bandwidth untuk mengakomodasi kebutuhan bisnis untuk akses kecepatan tinggi, penyimpanan data dan aplikasi. Penyedia layanan harus memiliki kemampuan load balancing yaitu kemampuan untuk memastikan bahwa sistem tidak kelebihan beban dan layanan tidak ada *delay* (penundaan)

4. Skalabilitas

   Dengan tidak adanya kendala pada kapasitas, komputasi awan menawarkan fleksibilitas dan skalabilitas yang lebih untuk kebutuhan teknologi informasi penggunanya.

5. Efisiensi

   Realokasi kegiatan manajemen operasional teknologi informasi ke layanan komputasi awan menawarkan kesempatan yang unik bagi pengguna untuk lebih memfokuskan pada inovasi, penelitian serta pengembangan bisnis. Hal tersebut memungkinkan terjadinya pertumbuhan bisnis dan produk serta bahkan dapat lebih menguntungkan dari sekedar keuntungan keuangan yang ditawarkan oleh layanan komputasi awan

6. Ketahanan

Penyedia layanan komputasi awan telah memiliki beberapa solusi yang dapat digunakan apabila terjadi bencana alam. Penyedia layanan memiliki ketahanan dan kapasitas untuk mematikan keberlanjutan layanan mereka walau terjadi hal yang tidak diduga. Seperti misalnya menempatkan server-server penyimpanan data di lokasi yang relatif aman dari gangguan dan kemampuan untuk mengaktifkan server cadangan apabila server utama mengalami gangguan atau sedang dalam pemulihan.

3.6 Masalah Keamanan Data Dalam Komputasi Awan

a. Masalah keamanan dari Virtual machine.

   Apakah Blue Cloud IBM atau Windows Azure di Microsoft, teknologi mesin virtual dianggap sebagai platform komputasi awan dari komponen fundamental, perbedaan antara Blue Cloud dan Windows Azure adalah bahwa virtual mesin berjalan pada sistem operasi Linux atau sistem operasi Microsoft Windows[136]. Teknologi virtual mesin membawa keuntungan yang nyata, ini memungkinkan pengoperasian server tidak lagi bergantung pada perangkat fisik. Tapi pada server virtual. Pada mesin virtual, perubahan yang fisik terjadi atau migrasi tidak mempengaruhi layanan yang diberikan oleh penyedia layanan. jika pengguna membutuhkan jasa lebih, penyedia dapat memenuhi kebutuhan pengguna tanpa harus memperhatikan perangkat keras fisik.

   Namun, *server virtual* dari kelompok server logis membawa banyak masalah keamanan. Pengamanan terhadap pusat data tradisional diukur pada platform perangkat keras, sementara komputasi awan mungkin merupakan server dari beberapa server virtual, server virtual mungkin milik kelompok server yang berbeda yang membawa server virtual pada banyak ancaman keamanan.

b. Keberadaan *super – user*.

[136]Herwin Anggeriana, dkk, Cloud Computing, hlm. 46

Untuk perusahaan yang menyediakan layanan komputasi awan (Cloud Computing), mereka memiliki hak untuk melaksanakan pengelolaan dan pemeliharaan data, adanya super-usersangat bermanfaat untuk menyederhanakan fungsi manajemen data, tetapi merupakan ancaman serius bagi pengguna pribadi. Dalam era privasi pribadi, data pribadi harus benar-benar dilindungi, dan fakta membuktikan bahwa platform Cloud Computing memberikan layanan pribadi dalam kerahasiannya. Bukan hanya pengguna individu tetapi juga organisasi memiliki potensi ancaman serupa, misalnya pengguna korporat dan rahasia dagang disimpan dalam platform komputasi awan mungkin dicuri. Oleh karena itu penggunaan hak super user harus dikendalikan di layanan komputasi awan.

c. Konsistensi data.

Lingkungan awan merupakan lingkungan yang dinamis, dimana pengguna data pengguna mentransmisikan data dari data center ke pengguna. Untuk sistem, data pengguna berubah sepanjang waktu. Membaca *(read*) dan menulis (*write*) data yang berkaitan dengan identitas otentikasi pengguna dan hal perijinan untuk mengakses data tersebut. Dalam sebuah mesin virtual, mungkin ada data pengguna yang berbeda 'yang harus wajib dikelola.Hal ini jelas bahwa kontrol akses tradisional, jelas sangat tidak cocok untuk lingkungan komputasi awan. Dalam lingkungan komputasi awan, mekanisme kontrol akses tradisional dianggap memiliki kekurangan serius.

Semua teknik keamanan data dibangun pada kerahasiaan, integritas dan ketersediaan dari tiga prinsip dasar. Kerahasiaan mengacu pada apa yang disebut dengan data aktual atau informasi yang tersembunyi, terutama pada daerah yang sensitive, kerahasian data berada pada persyaratan yang lebih ketat. Untuk komputasi awan, data disimpan di "pusat data", keamanan dan kerahasiaan data pengguna, merupakan hal yang penting.

Secara praktis, komputasi awan memberikan keuntungan karena sifat dasarnya menggunakan pusat data yang besar sehingga bisa menyebarkan sumber daya komputasi dengan biaya jauh lebih murah daripada menggunakan pusat data yang lebih kecil. Selain itu, permintaan penyatuan (pooling) dalam suatu pusat

data yang luas juga memungkinkan peningkatan pemanfaatan sumber daya, terutama dalam awan publik (public cloud). Penyedia sewa aplikasi yang multisewa dapat menghemat biaya tenaga kerja dan perawatan aplikasi. Komputasi awan juga menjanjikan penawaran yang elastis dan ketangkasan yang memungkinkan berkembangnya solusi dan aplikasi baru.

Dengan menggabungkan semua solusi yang ada, kita bisa selalu terhubung pada fasilitas komputasi meski kita sedang berada di tengah laut, ataupun di dalam pesawat tanpa sambungan internet. Dan begitu kita terhubung melalui internet, maka kemampuan *client* juga diperlukan untuk segera melakukan sinkronisasi dengan layanan komputasi awan[137].

Tetapi pada akhirnya layanan komputasi awan bukanlah solusi untuk semua masalah teknologi informasi. Hal terbaik untuk memanfaatkan keunggulan komputasi awan adalah dengan menggabungkannya dengan aplikasi di sisi klien dan juga server milik sendiri (jika ada) . Dengan demikian kita akan mendapatkan banyak keuntungan dari semua fasilitas yang tersedia. Misalnya, kemampuan sisi klien untuk melakukan proses lokal sangat diperlukan pada saat sambungan internet terputus. Dan kemampuan server milik sendiri juga menjadi sangat penting jika terjadi masalah *bottleneck* pada jaringan internet[138]

[137]Tony Seno Hartono, "Komputasi Awan dan Segala Aspeknya", <http://www.detikinet.com/read/2011/10/26/093855/1752688/328/komputasi-awan-dan-segala-aspeknya> Diakses pada 30 November 2011

[138]Ibid

BAB 4
PERLINDUNGAN DATA PRIBADI DALAM KOMPUTASI AWAN (CLOUD COMPUTING) DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Komputasi awan, sebuah generasi baru di dunia teknologi informasi yang diprediksi akan mengubah dunia komputasi. Penyimpanan data dan layanan berbasis internet dengan cepat muncul untuk melengkapi model tradisional dalam menjalankan perangkat lunak dan data yang disimpan pada *PC desktop* dan *server*. Dalam istilah sederhana, komputasi awan adalah cara untuk meningkatkan pengalaman komputasi dengan memungkinkan pengguna untuk mengakses aplikasi perangkat lunak dan data yang disimpan di pusat data diluar daripada perangkat pengguna sendiri atau PC atau pada pusat data pribadi.

E-mail, pesan singkat, *software* bisnis dan manajemen web konten adalah beberapa dari antara banyak aplikasi yang dapat ditawarkan melalui lingkungan awan. Banyak aplikasi yang telah ditawarkan dari jarak jauh melalui internet selama beberapa tahun, yang berarti bahwa komputasi awan mungkin tidak akan terasa sangat berbeda dari layanan web saat ini untuk sebagian besar pengguna. Di lain sisi komputasi awan meningkatkan jumlah pertanyaan mengenai kebijakan penting mengenai bagaimana orang-orang, organisasi, dan pemerintah menangani informasi dan interaksi dalam lingkungan awan ini.

4.1 Potensi Isu Hukum Pada Komputasi Awan

4.1.1 Proteksi Privasi dan Keamanan Data Pribadi

Data pengguna komputasi awan tidak disimpan pada *server* mereka sendiri, melainkan diakses melalui internet dari perangkat seperti laptop atau ponsel. Survei menemukan bahwa 90% dari pengguna komputasi Awan mengatakan bahwa mereka akan sangat khawatir jika perusahaan di mana data mereka disimpan menjualnya kepada pihak lain[139]. 80% mengatakan mereka akan sangat khawatir jika perusahaan menggunakan foto mereka dalam kampanye

[139] Minamur Chowdhury, "Cloud Computing : Facts, Security and Legal Challenges" (University of British Columbia Term Paper , December 2009) Hlm. 14

pemasaran[140]. 68% dari pengguna mengatakan mereka akan sangat khawatir jika perusahaan yang menyediakan layanan komputasi awan menganalisis informasi yang mereka berikan dalam rangka untuk menampilkan iklan yang relevan[141].

Data dan perlindungan privasi sangat penting untuk membangun kepercayaan pelanggan yang diperlukan untuk komputasi awan untuk mencapai potensi layanan sepenuhnya. Jika penyedia mengadopsi kebijakan yang lebih baik dan lebih jelas dan praktek, pengguna akan lebih mampu menilai risiko-risiko terkait yang mereka hadapi. Untungnya, banyak penyedia yang telah memiliki komitmen untuk mengembangkan kebijakan dan *best-practices* untuk melindungi data pelanggan dan privasi[142].

Kemudian adalah bagaimana jika *data center* terkena bencana? Adalah mungkin terjadi bahwa lokasi penyedia layanan komputasi awan adalah rentan terpengaruh karena bencana. Dalam publikasi 10-K dari Google Inc dengan *United States Securities and Exchange Commission* menyebutkan risiko seperti:

"The availability of our products and services depends on the continuing operation of our information technology and communications systems. Our systems are vulnerable to damage or interruption from earthquakes, terrorist attacks, floods, fires, power loss, telecommunications failures, computer viruses, computer denial of service attacks, or other attempts to harm our systems. Some of our data centers are located in areas with a high risk of major earthquakes. Our data centers are also subject to break-ins, sabotage, and intentional acts of vandalism, and to potential disruptions if the operators of these facilities have financial difficulties. Some of our systems are not fully redundant, and our disaster recovery planning cannot account for all eventualities. The occurrence of a natural disaster, a decision to close a facility we are using without adequate notice for financial reasons, or other unanticipated problems at our data centers could result in lengthy interruptions in our service. In addition, our products and services are highly technical and complex and may contain errors or vulnerabilities".[143]

[140] Ibid

[141] Ibid

[142] Alex Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services" (Journal of Medical Internet Research, 2011)

[143] Annual Report Form 10-K Google Inc and United States Securities and Exchange Comission. <http://investor.google.com/documents/20101231_google_10K.html> Comission file number 000-50726. Diakses pada 27 Agustus 2011. Hlm 52

Kemudian apakah ada cakupan kewajiban untuk pelanggaran privasi? Jika terjadi pelanggaran privasi karena kesalahan penyedia layanan awan, apakah ada cakupan kewajiban yang harus diambil atau dibayar oleh penyedia layanan kepada pengguna? Kemudian apa yang dapat dilakukan jika pusat data diretas? Meskipun semua vendor awan mencoba yang terbaik untuk melawan dan menangkis serangan hacker, tetapi jika *data center* dapat diretas, apakah konsumen dapat menuntut penyedia layanan untuk mengklaim adanya kehilangan keuntungan?

4.1.2 Hak Kekayaan Intelektual

Sifat komputasi awan adalah melakukan *outsourcing* infrastruktur teknologi informasi oleh pelanggan ke penyedia layanan komputasi awan[144]. Dalam beberapa perjanjian layanan, penyedia layanan awan mungkin memiliki pilihan (dan mungkin memang memiliki kebutuhan) untuk menggunakan penyedia layanan pihak keempat atau kelima dalam rangka untuk memenuhi permintaan untuk sumber daya komputasi awan.

1. Dalam konteks hukum paten, distribusi kepada pihak ketiga beberapa informasi rahasia yang berkaitan dengan invensi melalui pengaturan komputasi awan menimbulkan setidaknya masalah teoritis, apakah distribusi melalui awan tersebut merupakan bentuk dari suatu "*public knowledge*".[145]

2. Dalam konteks merek dagang, tampaknya ada pertumbuhan jumlah merek dagang yang menggabungkan komputasi awan. Istilah komputasi awan pertama kali diajukan sebagai merek adalah pada tahun 1997, tetapi akhirnya ditinggalkan[146].

3. Rahasia dagang melindungi secara hukum informasi eksklusif yang memiliki nilai ekonomi dan belum diungkapkan kepada publik. Seorang

[144] Peter Kang, "Intellectual Property and Legal Issues Surrounding Cloud Computing" (Makalah disampaikan pada seminar teleconference "Protecting IP Rights and Mitigating Infringements Risks in Virtual Storage and Applications oleh Strafford Publications, 12 Oktober 2011) Hlm. 14

[145] Ibid. Hlm 20

[146] Ibid.

pemilik rahasia dagang harus telah mengambil langkah-langkah yang wajar untuk melindungi informasi dari pengungkapan untuk memperoleh rahasia dagang ini[147]. Persyaratan ini sangat penting dalam bisnis ketika menyimpan data ke dalam komputasi awan. Pertanyaan muncul bagaimana penyedia layanan komputasi awan melindungi rahasia dagang tersebut? Pada pertemuan American Bar Association baru-baru ini, Sharon Sandeen, seorang profesor hukum Universitas Hamline, membahas bagaimana banyak penyedia layanan komputasi awan menolak bertanggung-jawab untuk keamanan dan enggan "untuk menegosiasikan syarat khusus yang menjadi bukti kewajiban kerahasiaan untuk tujuan rahasia dagang. Jika tidak ada kewajiban kerahasiaan disini, maka pelaku bisnis mungkin akan mengabaikan perlindungan rahasia dagang. Perusahaan dan pelaku bisnis harus belajar segala sesuatu yang mereka dapat tentang penyedia layanan komputasi awan wan sebelum memberikan informasi rahasia bisnis kepada penyedia layanan

4. Dan dalam konteks hak cipta, komputasi awan potensial menimbulkan masalah hukum di bidang data yang tersimpan dalam "awan" seperti program komputer. Dalam lingkungan komputasi awan, data dan informasi dapat dipisah dan disalin di beberapa lokasi terpisah[148].

Dan untuk semua bidang hak kekayaan intelektual, juga terdapat isu-isu *extraterritoriality* yang dapat timbul. Sebagai contoh, jika seseorang yang melanggar suatu karya, seperti perangkat lunak, yang kemudian telah disalin di awan atau disimpan di *server* di luar negeri, akan ada muncul pertanyaan apakah tindakan ini merupakan pelanggaran yang dapat dijangkau oleh hukum hak kekayaan intelektual masing-masing negara?[149]

4.1.3 Yurisdiksi Data

[147] David J. Shannon, " Storage of Trade Secrets in Cloud Computing", <http://www.databreachlegalwatch.com/2011/05/storage-of-trade-secrets-in-cloud-computing/> Diakses pada 11 Desember 2011

[148] Peter Kang. Intellectual Property and Legal Issues Surrounding Cloud Computing. Hlm 21

[149]. Hlm. 21

Dalam layanan *public cloud*, penyedia layanan komputasi awan mungkin tidak tahu di mana data yang secara fisik disimpan, bahkan mungkin tidak disimpan di negara yang sama[150]. Ini dapat menjadi masalah hukum ketika pihak yang terkait dengan data tersebut memerlukannya untuk mempertahankan kendali atas datanya tersebut[151]. Konflik hukum terjadi karena inti dari komputasi awan adalah Internet, dimana sifat dari internet yang *cross-border* dan multinasional[152]. Ketidakpastian yurisdiksi telah menyebabkan beberapa regulator untuk menerapkan sistem komputasi awan yang dapat menciptakan risiko yang tidak dapat diterima. *Director of Technology Risk* pada *Monetary Authority of Singapore* telah menyatakan bahwa "tidak mungkin untuk memungkinkan bank untuk menempatkan data pelanggan ke dalam awan tanpa due diligence yang signifikan, mengingat bahwa di Singapura perilaku tersebut bisa dihukum dengan hukuman penjara tiga tahun dan denda besar dan kuat"[153]. Pengguna potensial juga memiliki perhatian terhadap hal ini. Mereka khawatir bahwa layanan komputasi awan bisa menempatkan data-data bisnis mereka menjadi beresiko karena mereka bisa menjadi tunduk pada hukum asing atau tidak dapat diterima oleh hukum asing. Seperti contoh bahwa banyak pengguna khawatir bahwa penyedia komputasi menggunakan penyedia layanan komputasi awan yang terletak di Amerika Serikat atau yang mengoperasikan server di Amerika Serikat dapat mengakibatkan data mereka berisiko terhadap penggeledahan tanpa surat berdasarkan *US Patriot Act*[154]

4.2 Beberapa Kasus Pembobolan Data Pribadi Konsumen

[150] Ian Mitchell,dkk, "The Fujitsu White Book of Cloud Computing : The Definitive Guide to a Business Technology Revolution", Hlm. 20 . Dapat diakses di https://sp.ts.fujitsu.com/dmsp/docs/wp-cloud-adoption1.pdf

[151] Ibid.

[152] C. Ian Kyer dan Gabriel M.A Stern, "Where in the World is My Data? Jurisdictional Issues with Cloud Computing" (Fasken Martineau, 2011), hlm 3

[153] Stephen Withers, "Singapore Regulator Casts Doubt on Banking Clouds",<http://www.itnews.com.au/News/235977,singapore-regulator-casts-doubt-on-banking-clouds.aspx> Diakses pada 12 Desember 2011

[154] C. Ian Kyer dan Gabriel M.A Stern, "Where in the World is My Data? Jurisdictional Issues with Cloud Computing", Ibid.

4.2.1. Sony Corp (April 2011)

Sony Corp mengaku bahwa para peretas (hacker) berhasil menjebol data pribadi milik puluhan juta konsumen mereka yang tergabung dalam jaringan game online PlayStation dan layanan film mereka, serta konsumen layanan musik digital Sony, Qriocity[155]. Sony memastikan bahwa cracker juga telah menjebol database konsumen *Sony Online Entertainment*. *Database* yang dijebol termasuk 12.700 data kartu kredit konsumen dari tahun 2007, serta data kartu debet milik 12.700 konsumen[156].

Pelanggaran data yang menimpa lebih dari 100 juta *PlayStation Network* dan account pengguna *Sony Online Entertainment* mungkin akan menjadi pelanggaran data yang paling mahal dari semua waktu[157]. Sony menyatakan bahwa informasi dari 77 juta PlayStation Network account pengguna bisa dicuri. *Hacker* mencuri data pribadi pengguna *Sony Online Entertainment*, termasuk informasi kartu kredit dan debet dalam serangan kompleks yang bisa menghabiskan biaya Sony dan kartu kredit Emiten $1 hingga $2 miliar. Sampai saat ini, pembobolan data terbesar adalah antara lain pembobolan 130 juta nomor kartu kredit yang dicuri dari Heartland Payment System pada tahun 2008, hingga 100 juta account dari retailer TJX pada tahun 2005 dan 2006, dan lebih dari 4,2 juta nomor kartu kredit dan debit dari took Hannaford Bros. pada 2008.

Larry Ponemon, chairman *Ponemon Institute*, mengatakan bahwa pelanggaran data dari Sony akan lebih mahal dari kasus-kasus pembobolan data sebelumnya. Sony mengumumkan pada hari Senin bahwa informasi pribadi dari account pengguna SOE hingga 24.6 juta bisa telah dicuri, dan bahwa kartu kredit, kartu debit, atau nomor rekening bank dicuri dari lebih dari 20.000 pengguna di luar Amerika Serikat.

---

[155] "77 Juta Data Konsumen Sony PlayStation Dibobol", <http://fokus.vivanews.com/news/read/216981-77juta-data-pengguna-sony-playstation-dibobol> Diakses pada 6 Desember 2011

[156] "Ribuan Data Penting Konsumen Sony Bobol", <http://fokus.vivanews.com/news/read/218210-lagi--12-ribu-data-konsumen-sony-bobol> Diakses pada 6 Desember 2011

[157] Mary Helen Miller, "Sony Data Breach Could Be Most Expensive Ever", <http://www.csmonitor.com/Business/2011/0503/Sony-data-breach-could-be-most-expensive-ever> Diakses pada 6 Desember 2011

Hanya lebih dari empat bulan setelah memulihkan sepenuhnya jaringan PlayStation dari serangan *hacker* yang melumpuhkan mereka pada April lalu, *Cyber Security Chief* baru Sony Phillip Reitinger mengumumkan di blog PlayStation[158] bahwa *hacker* kembali. Tetapi itu tidak seburuk dibandingkan dengan serangan pertama. Sony telah mengungkapkan bahwa *hacker* kembali berhasil menginvasi jaringan online perusahaan game, menembus 93.000 rekening. Serangan ini tampaknya terlibat informasi yang diperoleh dari situs pihak ketiga

4.2.2 Google Android (Mei 2011)

Google memakai *patch* di sistem operasi *Android* yang terdapat cacat pada bagian keamanan yang mengakibatkan kontak dan kalender data melalui jaringan Wi-Fi (wireless fidelity) terbuka adalah sangat riskan untuk dibobol[159]. Masalah terletak pada cara Android menangani token otentikasi.Jika data tersebut dikirim melalui sambungan yang tidak aman (*http*), *hacker* pada jaringan Wi-Fi yang sama sebagai pengguna bisa dibayangkan mencuri otentikasi dan mendapatkan akses ke pengguna kalender, kontak dan *Picasa Web Album*. Meskipun masalah kebocoran kontak dan kalender sudah diperbaiki di Android 2.3.4, mayoritas Android ponsel masih menjalankan versi perangkat lunak.

Beberapa *software Google Android* menggunakan metode yang disebut *ClientLogin* untuk mengotorisasi transfer data sensitif ke layanan berbasis Web. *ClientLogin* menggunakan token otorisasi untuk lulus pengguna login dan

[158]Philip Reitinger, "An Important Message From Sony's Chief Information Security Officer", <http://blog.eu.playstation.com/2011/10/12/an-important-message-from-sonys-chief-information-security-officer/> Diakses pada 7 Desember 2011

[159] Jared Newman, "Google Issues Patch to Plug Android Data Leaks", <http://www.pcworld.com/article/228146/google_issues_patch_to_plug_android_data_leaks.html > Diakses pada 6 Desember 2011

password melalui sambungan aman (*https*)[160] untuk layanan Web, seperti Google Calendar atau sinkronisasi kontak anda[161]

Masalahnya, menurut para peneliti di Universitas Ulm Institute of Media Formatics, terjadi setelah token divalidasi dan kembali dan kemudian dapat digunakan untuk hingga dua minggu pada permintaan melalui koneksi jaringan http yang tidak aman, yang membuatnya rentan terhadap pencurian dari hacker melalui jaringan Wi-Fi. Hacker bisa menggunakan token yang dicuri untuk mendapatkan akses ke kalender, kontak, atau Picasa gambar. *Hacker* kemudian bisa mencuri atau memodifikasi informasi dalam layanan ini.

4.2.3 SEGA (Juni 2011)

Setelah PlayStation, giliran Sega Corp yang menjadi sasaran penjahat *cyber*. *Developer video game* asal Jepang itu memastikan bahwa data sekitar 1,3 juta penggunanya telah dibobol dari *database*[162].*Database* yang berhasil dicuri itu berisi mulai dari nama, tanggal lahir, alamat email, *username* dan *password* dari layanan online Sega Pass. Namun belum diketahui apakah data yang berhasil dicolong itu termasuk data kartu kredit. Hingga saat ini, Sega menyatakan belum ada informasi terkait kerugian finansial. Namun Sega mengakui, jika data kartu kredit yang berhasil dicuri pelaku, tentu akan menjadi lebih mengkhawatirkan. Untuk mengantisipasinya, Sega telah menghentikan untuk sementara waktu layanan Sega Pass. Sebab jika data kartu kredit juga berhasil dicuri pelaku, tentu ini akan menjadi lebih mengkhawatirkan. Sega sendiri sudah mematikan layanan Sega Pass untuk sementara waktu.

---

[160] Hypertext Transfer Protocol Secure (HTTPS) adalah kombinasi dari Hypertext Transfer Protocol (HTTP) dengan protocol SSL / TLS untuk menyediakan komunikasi yang terenkripsi dan menandakan sebuah jaringan atau web adalah aman. Koneksi HTTPS sering digunakan untuk transaksi pembayaran di World Wide Web dan untuk transaksi sensitif dalam sistem informasi perusahaan

[161] Jared Newman, "Researchers Discover Android Data Leaks : What You Need to Know, <http://www.pcworld.com/article/228045/researchers_discover_android_data_leaks_what_you_need_to_know.html> Diakses pada 6 Desember 2011

[162] Ardhi Suryadi, "1,3 Juta Data Pengguna SEGA Dicuri", <http://www.detikinet.com/read/2011/06/20/092356/1663626/323/13-juta-data-pengguna-sega-dicuri/> Diakses pada 6 Desember 2011

Sega Pass, yang langsung menangguhkan jasa permainan, meminta maaf kepada para pengguna atas kebocoran keamanan tersebut dan berharap bisa segera kembali menjalankan sistem. Sega merekomendasikan para pengguna untuk membuat kata kunci baru, terutama jika data-data mereka digunakan untuk jasa-jasa lain. Penyelidikan sedang dilakukan untuk mengidentifikasi pelaku gangguan tersebut[163]

4.2.4 Citigroup Inc. (Juni 2011)

Sekitar 200 ribu data nasabah kartu kredit Citibank di Amerika Utara dicuri identitasnya oleh *hacker*. Peretas yang masuk ke situs rekening Citi online itu berhasil mencuri identitas nama, nomor rekening, dan alamat email[164]. Seperti dilansir Associated Press, Citigroup Inc menemukan sekitar 1 persen dari pemegang kartu kredit datanya diketahui oleh *hacker*. Menurut laporan 2010, Citi memiliki lebih dari 21 juta pelanggan kartu kredit di Amerika Utara. Bank berbasis di New York ini tidak mengatakan berapa tepatnya akun yang dicuri. Namun, Citi mengatakan pihaknya telah menghubungi para nasabah[165].

Citi menjelaskan bahwa *hacker*itu tidak mampu mendapat akses ke nomor jaminan sosial, data tanggal lahir, tanggal kadaluarsa kartu atau kartu kode keamanan. Informasi ini pentingterutama terkait pada kejahatan pemalsuan identitas.Penjahat *cyber* biasanya menguras akun bank dan mengajukan permohonan kartu kredit ganda, sehingga nasabah Citi dianggap rentan terhadap hal ini. Regulator perbankan di Amerika Serikat meminta bank untuk meningkatkan keamanan. Pencurian data nasabah Citibank ini merupakan pelanggaran baru setelah serangan peretas terhadap sejumlah perusahaan besar

4.3. Urgensi Aspek Perlindungan Data Pribadi di Indonesia

[163] "Peretas Bobol Data Pengguna Perusahaan Permainan SEGA", <http://www.pikiran-rakyat.com/node/149206> Diakses pada 6 Desember 2011

[164] "Data 200 Ribu Nasabah Citibank AS Dicuri", <http://bisnis.vivanews.com/news/read/225917-data-200-ribu-nasabah-citibank-dicuri-di-as> Diakses pada 7 Desember 2011

[165] Ibid

4.3.1 Pengaruh Instrumen Hukum Internasional Terhadap Perlindungan Data Pribadi di Indonesia

Instrumen hukum internasional memiliki peran penting bagi Indonesia. Indonesia sebagai bagian dari masyarakat internasional, dimana instrumen internasional sebagai salah satu sumber hukum dalam mengatur hubungan atau kerjasama antara negara. Melalui perjanjian internasional, setiap negara menyelenggarakan berbagai kegiatan atau menyelesaikan berbagai masalah yang terjadi antara negara. Tidak ada satupun negara yang tidak memiliki perjanjian dengan negara lain karena itu adalah penting untuk memiliki posisi politik atau ekonomi di masyarakat. Salah satu upaya untuk mendorong perdagangan, investasi dan akses pasar sedang melakukan upaya ambisius untuk memberlakukan privasi dan perlindungan data pribadi.

Uni Eropa merupakan salah satu negara terkemuka dengan privasi yang kuat dan data pribadi perlindungan membatasi transfer data setiap warga negara mereka ke negara yang tidak memiliki tingkat perlindungan data yang setara. Jadi, jika Indonesia ingin memiliki kerjasama yang baik dengan negara-negara Eropa, Indonesia harus mempersiapkan perlindungan data pribadi dan privasi yang memadai dalam sistem hukumnya. Ini akan menjadi alasan baik bagi pemerintah Indonesia untuk meningkatkan perlindungan data ke depannya. Dan juga dengan AS, mereka memiliki perlindungan yang kuat untuk warga negara mereka, sehingga jika Indonesia ingin memiliki kerjasama yang kuat dengan Amerika Serikat, lebih baik bagi Indonesia untuk memiliki privasi dan perlindungan data dalam sistem hukum Indonesia.

Terkait dengan privasi dan perlindungan data, Indonesia tidak mengambil bagian dalam privasi dan perlindungan data instrumen internasional. Negara-negara Asia seperti Jepang, Singapura, Korea Selatan dan Cina adalah negara terkemuka di ranah privasi dan perlindungan data pribadi yang menjalin hubungan baik dengan Indonesia. Sebagai kekuatan yang muncul dari Asia, Indonesia perlu mempertimbangkan peran mereka dalam melindungi warga negara mereka.Saat ini karena hukum Indonesia dapat meratifikasi instrumen hukum internasional maka Indonesia memiliki dasar hukum untuk membuat hukum internasional yang berlaku di tingkat nasional. Indonesia telah menandatangani pedoman OECD

(*Organisation for Economic Co-operation and Development*) Guidelinespada tahun 2004, dan mengikuti pedoman untuk menegakkan penerapan regulasi privasi dan perlindungan data. Sebagai anggota APEC (*Asia-Pacific Economic Cooperation*), Indonesia mengikuti Apec Privacy Framework 2004, yang dengan jelas menyebutkan dalam kata pengantar, *"the potential of electroniccommerce cannot be realized without government and business cooperation todevelop and implement technologies and policies, which build trust and confidence insafe, secure and reliable communication, information and delivery systems, andwhich address issues including privacy…"*. Keanggotaan ini mendorong legislasi nasional masing-masing negara anggota untuk mengenali perlindungan privasi untuk keseimbangan dan mempromosikan informasi yang efektif dalam rangka untuk mempromosikan kerjasama ekonomi terutama dalam perdagangan elektronik antara anggota.

Uni Eropa merupakan pasar yang sangat menarik bagi Indonesia karena ini adalah pasar terbesar untuk ekspor non minyak dan gas dan juga investor Eropa telah terbukti menjadi yang paling stabil dan mitra yang dapat dipercaya dari Indonesia. Jadi, adalah penting bagi Indonesia untuk memecahkan tantangan dan hambatan yang mereka hadapi ketika melakukan bisnis lintas perbatasan. Dengan kata lain, penting ke Indonesia untuk mengisi kebutuhan di tingkat Uni Eropa pada standar privasi dan perlindungan data.

Tidak hanya karena alasan ekonomi, kebijakan privasi harus diperkenalkan sebagai bagian dari hukum mengenai hak asasi manusia. Privasi merupakan bagian dari hak asasi manusia dan perlindungan data pribadi merupakan salah cara untuk menghormati hak ini. Di Indonesia, ada kecemasan tentang perlindungan untuk privasi dan perlindungan data karena belum ada undang-undang yang secara jelas dan spesifik mengatur hal tersebut. Oleh karena itu, privasi dan masalah perlindungan data pribadi telah menjadi agenda mendesak di era modern saat ini. Banyak negara telah menerapkan perlindungan hukum bagi data pribadi, tetapi tidak ada hukum Indonesia yang telah ditetapkan dengan kuat untuk hal ini. Peningkatan dan pengembangan ilmu pengetahuan dan teknologi, globalisasi, dan kekuatan media telah sangat mendesak akan kebutuhan untuk privasi dan perlindungan data pribadi.

Hambatan untuk privasi dan perlindungan data regulasi berasal dari sejarah bangsa Indonesia sendiri. Sebagai sebuah negara Asia, Indonesia menemukan sangat sulit untuk menentukan dan mengatur privasi. Sebagian besar negara Asia telah tidak tahu menahu tentang privasi. Privasi belum dilihat sebagai masalah "serius" dalam Asia, termasuk Indonesia. Kebanyakan orang Asia tinggal tradisional dalam masyarakat komunal, yang tidak menaruh banyak perhatian untuk privasi. Istilah privasi sebagai hak asasi manusia berasal dari dunia barat dan menjadi penting di era teknologi informasi dan komunikasi (TIK).

Dalam penelitian ini penulis telah membandingkan pengaturan perlindungan data pribadi dalam *EU Directive95/46/EC*dan *Malaysian Personal Data Protection Act* dengan beberapa pengaturan di peraturan perundang-undangan Indonesia sebagai berikut :

Isu Hukum	**Instrumen Internasional (Uni Eropa dan Malaysia)**	**Pengaturan di Indonesia**
Pemberitahuan	Pasal 6 Directive 95/46/EC ; Pasal 7 Malaysia PDP Act	Pasal 21 UU 39 Tahun 1999, Peraturan Bank Indonesia No. 7/6/PBI/2005, Pasal 26 UU No. 11 Tahun 2008
Batasan Pengumpulan Data Pribadi	Pasal 6 Directive 95/46/EC; Pasal 10 Malaysia PDP Act	Tidak ada pengaturan khusus
Penggunaan Data Pribadi	Pasal 6 Directive 95/46/EC; Pasal 7 Malaysia PDP Act	Pasal 49 UU No. 8 Tahun 1981
Pilihan	Pasal 12 Directive 95/46/EC; Pasal 7 Malaysia PDP Act	Tidak ada pengaturan khusus
Tujuan Penggunaan Data	Pasal 6 Directive 95/46/EC; Pasal 8 dan	Pasal 49 UU No. 8 Tahun 1981

	Pasal 10 Malaysia PDP Act	
Kewajiban Menjaga Keamanan Data	Pasal 6 Directive 95/46/EC, Pasal 9 Malaysia PDP Act	Pasal 42 UU No. 36 Tahun 1999, Pasal 57 UU No. 36 Tahun 2009, Pasal 26 UU No. 11 Tahun 2008, Pasal 47 UU No. 29 Tahun 2004, Pasal 40 ayat (1) UU No. 10 Tahun 1998
Hak Akses dan Memperbaiki	Pasal 12 Directive 95/46/EC; Pasal 12 Malaysia PDP Act	Pasal 28F Undang-Undang Dasar 1945
Partisipasi Individu	Pasal 15 Directive 95/46/EC; Pasal 12 Malaysia PDP Act	Tidak ada pengaturan khusus

4.3.2 **Analisis Hubungan Pasal Perlindungan Data Pribadi Dalam Undang-Undang Informasi dan Transaksi Elektronik dengan Praktik Komputasi Awan**

Belakangan ini masyarakat Indonesia cukup resah dengan adanyafenomena "kebocoran data" yang menyebabkan mengemukanya beragamkasus semacam beredarnya dokumen rahasia Wikileaks, SMS penawaran kredit, gambar/videoporno, nomor kartu kredit, data/informasi rahasia perusahaan, dan lain sebagainya. Inti permasalahan tentang kebocoran data konsumen terletak pada beberapa kesalahan berpikir yang perlu segera dikoreksi.[166]. Data pribadi saat ini adalah suatu aset yang berharga untuk bisnis dan organisasi yang terus-menerus mengumpulkan, bertukar, mengolah, menyimpan dan bahkan menjual

[166]Richardus Eko Indrajit, "Fenomena Kebocoran Data : Mencari Sumber Penyebab dan Akar Permasalahannya". Makalah dapat diunduh di <http://www.idsirtii.or.id/content/files/IDSIRTII-Artikel309-FenomenaKebocoranData.pdf>

data pribadi sebagai komoditas, terutama yang berkaitan dengan konsumen. Dalam lingkungan jaringan, sejumlah besar data pribadi sekarang dapat dikumpulkan dari pengguna internet dan dikumpulkan untuk membuat profil dari aktivitas *online* mereka dan preferensi. Dan dalam beberapa kasus, koleksi dan agregasi dapat berlangsung tanpa sepengetahuan pemilik data. Dalam dunia jaringan, menjamin privasi konsumen jauh lebih sulit dibandingkan dengan dunia fisik.

Kompilasi data dari vendor keamanan komputer memperkirakan bahwa pada saat ini terjadi satu pencurian identitas dalam setiap 3 detik atau setara dengan 10 juta informasi pribadi per tahun dan terus meningkat kecepatan pertumbuhannya maupun jumlah/volumenya[167]. Informasi identitas personal yang bersifat umum seperti jenis kelamin, umur, alamat, email dan pekerjaan serta data rahasia seperti nomor rekening bank dan data finansial adalah komoditas yang paling diminati di pasar *underground*[168]. Para pemasar yang hendak melakukan market profiling membutuhkan data semacam ini yang apabila dikumpulkan melalui prosedur biasa akan memakan waktu dan biaya tidak sedikit. Sehingga penawaran dari pasar tidak resmi bisa menjadi pilihan yang rasional bagi sebagian perusahaan. Kebutuhan serupa juga berkembang terutama untuk tujuan targetted attack kepada tokoh masyarakat yang populer dan aktif di jejaring sosial. Tujuan serangan adalah *fraud*[169].

Tahun 2010 terjadi sejumlah pencurian informasi pribadi dan pembajakan akun yang berujung ke modus *fraud* menimpa tokoh masyarakat seperti artis, politisi dan pejabat negara. Di tahun 2011 jenis ancaman dan serangan ini akan semakin meningkat karena pengungkapan kasus selama ini hampir tidak ada karena terkendala sulitnya pelacakan secara legal formal[170].

---

[167] M. Salahuddien, " Tren Keamanan Internet Indonesia 2011" , Makalah dapat diunduh di website resmi Indonesia Security Incident Response Tean on Internet Infrastructure (ID-SIRTII) <http://idsirtii.or.id/content/files/artikel/TREN%20KEAMANAN%20INTERNET%20INDONESIA%202011.pdf>

[168] Ibid

[169] Ibid.

[170] Ibid.

Kewajiban menyerahkan data pribadi, yang menyangkut banyak aspek kehidupan dan perjalanan hidup seseorang dan bahkan keluarganya, telah menjadikan individu tawanan sistem. Data pribadi harus diserahkan untuk kebutuhan apapun, mulai dari mengajukan kredit rumah, melamar pekerjaan, mengambil hasil undian, dan sebagainya. Sebaliknya, seakan tidak ada kewajiban dari pihak yang menghimpun data pribadi tersebut untuk menjaga kerahasiaannya, dalam pengertian hanya menggunakannya untuk kepentingan seperti yang telah disepakati. Sering terjadi, data pribadi itu diteruskan kepada pihak lain tanpa seizin pribadi yang bersangkutan. Misalnya, bagaimana sebuah perusahaan bisa menawarkan produk atau jasanya kepada seseorang dengan mengirim surat ke alamat rumah padahal nama dan alamat yang bersangkutan tidak tercantum di buku telepon.

Ada berbagai kategori data pribadi. Kategori pertama adalah data pribadi yang terkait dengan orang-orang dalam organisasi bisnis; investor, direksi, karyawan, dan setiap mitra outsourcing atau bisnis. Siapapun yang memiliki akses ke data pribadi seperti misalnya mungkin dapat menilai posisi keuangan organisasi berdasarkan remunerasi keuangan bahwa individu memiliki. Kategori kedua data pribadi berhubungan dengan masyarakat luas, konsumen masa lalu, saat ini dan calon yaitu sebuah entitas bisnis. Data pribadi tersebut sangat penting untuk bisnis karena membantu mereka bentuk tujuan bisnis mereka dan strategi pemasaran produk mereka. Pertama, bahwa data (termasuk data pribadi) tidak seperti harta/aset yang memiliki sifat dan hak-hak terkait perlindungan properti (*property rights*). Kedua, bahwa hak melindungi kepentingan dan kehidupan pribadi bukan merupakan bagian dari hak asasi manusia. Kesalahan berpikir pada poin pertama akan mengakibatkan terjadinya penyalahgunaan data dan pengambilalihan (konversi) hak atas kepemilikan dan penggunaannya secara sewenang-wenang. Data yang diberikan oleh konsumen sebagai bagian dari proses penyediaan barang dan jasa akan dianggap hak milik penyedia jasa sehingga dapat digunakan tanpa izin atau pengetahuan pemilik asal data tersebut. Secara etis, data dan informasi yang diberikan oleh pengguna layanan kepada perusahaan yang meminta data pribadi hanya untuk keperluan perusahaan yang bersangkutan dan hanya untuk kepentingan tertentu seperti yang diinginkan

pemberi data. Dan, perusahaan penerima data tidak boleh mempublikasikan atau menjual data pribadi konsumen ke pihak ketiga.

Pengaturan perlindungan data pribadi yang secara spesifik dalam media elektronik terdapat dalam Pasal 26 Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 26

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Menurut Sonny Zulhuda, Ph.D dari International Islamic University Malaysia mengungkapkan bahwa UU No. 11 Tahun 2008 masih sangat tidak signifikan dalam mengatur penggunaan data pribadi karena pasal tersebut hanya merupakan ketentuan umum dan tidak menjelaskan berbagai isu yang banyak diperbincangkan di kancah internasional[171]. Pasal tersebut tidak secara jelas maksud dari "penggunaan" setiap informasi apakah termasuk kegiatan "pengumpulan", "pemrosesan", "penyimpanan", "diseminasi" dan sejenisnya. Kemudian menurut beliau terkait dengan persetujuan (*consent*) dimana penggunaan data harus dilakukan atas persetujuan orang yang bersangkutan apakah dalam pasal ini tergolong pada persetujuan implisit (*implied consent*) atau memang harus ada persetujuan eksplisit.

Kemudian menurut Donny Budhiyo Utoyo, S.Kom, *Executive Director* dari *ICT Watch* yang dihubungi penulis melalui forum DetikInet mengungkapkan bahwa UU ITE tidak secara khusus mengatur tentang *Cloud Computing*[172]. UU ITE lebih bicara tentang kepastian hukum atas segala transaksi dan komunikasi yang dihantarkan melalui media elektronik, khususnya yang berbasiskan *Internet Protocol* (IP). Dengan kepastian hukum tersebut, maka jika dibutuhkan aspek

[171]Sonny Zulhuda, "Data Privacy in Indonesia - Quo Vadis?", <http://sonnyzulhuda.wordpress.com/2011/01/25/adakah-perlindungan-data-konsumen-di-indonesia/>, Diakses pada 14 Januari 2012

[172]Donny BU, "Apakah UU ITE Lindungi Pengguna Cloud?" <http://www.detikinet.com/read/2011/11/14/125849/1766922/1205/apakah-uu-ite-lindungi-pengguna-cloud>, Diakses pada 29 Desember 2011

legalitas ataupun pembuktian atas data/bukti suatu transaksi/komunikasi yang melalui Internet, bukti elektronis/digital sudah dapat diakui oleh negara. Selain itu, UU ITE juga bicara aktivitas-aktivitas apa saja secara elektronis dan/atau melalui Internet yang dianggap dapat melanggar hukum dan dapat dikenakan sanksi. Selain UU ITE, Indonesia juga memiliki UU Telekomunikasi dan Peraturan Pemerintah turunannya yang juga mengatur tentang aktifitas elektronis. Menurut beliau terlepas dari pengaturan UU ITE, perlindungan data pelanggan seharusnya adalah berdasarkan itikad baik dan upaya maksimal dari para pihak, dalam hal ini pihak penyelenggara layanan dan penggunanya. Karena meskipun data pelanggan adalah hak privasi yang harus dilindungi dengan baik, kadangkala model bisnis atau layanan berbasiskan Internet yang abaikan atau tak sepenuhnya menghargai privasi tersebut.

Pendapat yang hampir sama dikemukakan oleh *Country Cloud Computing Leader* IBM Indonesia, Kurnia Wahyudi. Beliau mengungkapkan bahwa terkait dengan regulasi bagi komputasi awan adalah sebaiknya aspek teknologinya agar jangan terlalu diatur dengan undang-undang tetapi esensinya bagi penyedia layanan dan pengguna yakni aspek perlindungan data dan kelangsungan akses terhadap data bila sang penyedia tak dapat melanjutkan bisnisnya[173]. Beliau disini mengandaikan adanya perlindungan data bagi pengguna layanan elektronik seperti halnya perlindungan terhadap nasabah sebuah bank. Karena bagi sebuah perusahaan, data adalah tulang punggung kelangsungan bisnis perusahaan tersebut, karena di dalamnya ada data tagihan, data operasi perusahaan, dan lain sebagainya. Bapak Kurnia juga menyarankan agar Pemerintah untuk menerapkan perlindungan yang sama juga berlaku layaknya nasabah bank dengan LPSI (Lembaga Penjamin Simpanan Indonesia), dengan membentuk Lembaga Penjamin Data Indonesia (LPDI).

Sedangkan menurut Anggana Gunita, *Legal Officer* dari Biznet Networks mengungkapkan terkait dengan perlindungan data pribadi dalam UU ITE masih lemah khususnya bagi pihak penyedia layanan komputasi awan karena tidak jelas mengatur mengenai sejauh mana besaran ganti rugi yang bisa pengguna layanan

[173] Hasil wawancara dengan Country Cloud Computing Leader IBM Indonesia, Kurnia Wahyudi tanggal 14Desember 2011

gugat terhadap penyedia layanan[174]. Menurutnya hal tersebut tentunya menjadi suatu hambatan tersendiri. Beliau mencontohkan apabila suatu bank nasional atau kementerian pusat menggunakan layanan komputasi awan yang disediakan mereka kemudian suatu hari terjadi kebocoran data atau pusat data tidak bekerja dalam sekian waktu, maka kerugian yang ditanggung oleh bank dan kementerian tersebut sudah sangat besar dan apakah kerugian-kerugian tersebut semuanya dapat dibebankan pada penyedia layanan yang notabene perusahaan yang lebih kecil dari bank nasional atau kementerian tersebut.

Walau UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya mengatur satu pasal tentang Perlindungan Data Pribadi, namun pada perkembangannya Kementerian Komunikasi dan Informatika Republik Indonesia tengah menyiapkan aturan tentang keamanan dan privasi di *cloud computing*melalui draft Rancangan Peraturan Pemerintah (RPP) Penyelenggaraan Informasi dan Transaksi Elektronik (PITE)[175].

4.4. Tanggung Jawab Penyedia Layanan Komputasi Awan Terhadap Data Pengguna

Pada masa lalu data dan software komputer tidak termasuk dalam suatu hal yang dapat diterpakan prinsip *strict liability* karena data dan software dikategorikan sebagai *intangible asset*, namun ternyata hal tersebut justru telah mengakibatkan perkembangan industrinya menjadi negative bagi kepentingan perlindungan konsumen[176]. Penerapan tanggung jawab penyedia layanan komputasi awan disini bisa mengacu pada teori-teori tanggung jawab penyelenggara sistem elektronik.

Dalam praktik, jika pembuatan sistem tidak untuk digunakan sendiri, maka umumnya sistem tersebut adalah dibuat dalam rangka hubungan bisnisnya dengan

[174] Hasil wawancara dengan Legal Officer Biznet Networks, Anggana Gunita pada tanggal 16Desember 2011

[175]"Kominfo Siapkan Aturan Keamanan Cloud", <http://kominfo.go.id/liputan/detail/1742/Kominfo+Siapkan+Aturan+Keamanan+Cloud+Computing+> Diakses pada 3 Januari 2012

[176] Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, (Jakarta: Raja Grafindo Persada, 2010), hlm 225

pihak ketiga (konsumen). Dan dalam kelazimannya sebaiknya penyelenggara tidak lupa untuk mengasuransi sistem tersebut terlebih dahulu sebelum memutuskan untuk berhubungan dengan pelanggan. Berupaya sebaik mungkin untuk meminimalkan segala macam risiko (risk management) adalah kata kunci pertanggungjawaban penyelenggara kepada public, khususnya yang menjadi pelanggannya atau konsumennya.

Selain tanggung jawab kepada konsumen, penyelenggara juga bertanggung jawab untuk mengikuti standar yang lazim berlaku dalam komunitasnya dan/atau terhadap penerapan pedoman pemerintah sebagai patokan melakukan upaya yang terbaik dan menjaga mutu penyelenggaraan jasanya (*Quality of Services*). Pada dasarnya ia harus bertanggung jawab secara mutlak terhadap semua dampak kerugian yang ditimbulkannya kepada pihak lain, namun hal itu bisa berubah menjadi terbatas (pembatasan tanggung jawab), jika ada suatu mekanisme tertentu yang menjadi ukuran dalam *best practices.*

Dalam kaitannya dengan tanggung jawab hukum maka jika dipandang dari keberadaan suatu kewajiban baik sebelum atau setelah terjadinya suatu peristiwa tak tentu (*accident*), maka terhadap tanggung jawab hukum sebenarnya juga dapat dibedakan dalam dua hal, yakni : (i) tanggung jawab sebelum terjadi suatu kerjadian dan (ii) tanggung jawab setelah kejadian[177].

Tanggung jawab sebelum suatu kejadian (*ex-ante liability*) adalah tanggung jawab untuk mematuhi semua UU dan/atau regulasi administrasi negara dalam rangka memberikan suatu yang layak kepada publik[178]. Sementara untuk tanggung jawab setelah kejadian (*ex-post liability*) adalah tanggung jawab untuk memulihkan keadaan bagi yang dirugikan kepada keadaan yang semula. Kepentingan tersebut direpresentasikan dengan pembayaran sejumlah ganti rugi yang sesuai dengan kerugian yang diderita, sebagai bentuk kompensasi dari perbuatan tersebut[179]

[177] Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Hlm. 159

[178]Ibid, Hlm 160

[179]Ibid.

Dalam penelitian ini penulis berhasil untuk mewawancarai Bapak Tony Seno Hartono, National Technology Officer Microsoft Indonesia ; Bapak Kurnia Wahyudi, Country Cloud Computing Leader IBM Indonesia dan Ibu Anggana Gunita, Legal Officer PT Supra Primata Nusantara (Biznet Networks) untuk mendapatkan informasi yang lebih dalam mengenai tanggung jawab dari penyedia layanan komputasi awan dalam melindungi data pribadi pengguna layanan komputasi awan.

Ada 4 (empat) permasalahan terkait dengan tanggung jawab penyedia layanan komputasi awan yang ingin diketahui yaitu:

1. Pihak yang memiliki otentikasi atau akses kontrol kepada data pelanggan
2. Lokasi pusat data pelanggan disimpan.
3. Tindakan yang dilakukan oleh penyedia layanan komputasi awan untuk melindungi data pelanggan.
4. Pertanggung jawaban dari penyedia layanan komputasi awan apabila data pelanggan tersebut bocor atau disalahgunakan.

4.4.1 Pihak yang Memiliki Autentikasi atau Akses Kontrol Kepada Data Pelanggan

Pertanyaan ini terlontar untuk menjawab kekhawatiran pengguna layanan komputasi awan tentang siapa saja pihak yang dapat memiliki akses terhadap data yang mereka tempatkan dalam komputasi awan. Terkait dengan autentikasi atau akses kontrol terhadap data pelanggan, Tony Seno menyebutkan bahwa pada layanan Microsoft terdapat 2 (dua) tipe autentikasi yang dibedakan berdasarkan lokasi server yaitu apabila layanan awan tersebut berada atau dengan server di Microsoft maka kontrol akses dan autentikasi ada di Microsoft dan apabila layanan awan tersebut berada atau dengan server di mitra Microsoft (misalnya Telkom atau Infinys) maka kontrol akses dan autentikasi ada di perusahaan-perusahaan tersebut.

Kemudian dalam layanan IBM Cloud Computing, Kurnia Wahyudi menjelaskan bahwa secara umum, sesuai teknologi cloud yang diterapkan oleh IBM dalam bentuk *secured multi-tenancy*, maka akses terhadap isi (content) data pelanggan hanya dapat diakses dan dikontrol oleh pelanggan yang bersangkutan.

Bahkan Admin Cloud Provider, tidak dapat mengakses data tersebut menurut beliau.

Sedangkan dalam layanan Biznet Cloud Computing sendiri terdapat 2 (jenis) layanan yaitu *Manage Service* dan *Non-Manage Service*, dimana dalam *Manage Service*, Biznet sebagai penyedia layanan komputasi awan akan melakukan *total service* terhadap pemeliharaan layanan komputasi awan yang telah disewa oleh pelanggan, sedangkan *Non-Manage Service* adalah dimana pelanggan memiliki kontrol penuh untuk menggunakan layanan komputasi awan yang telah disediakan. Menurut Anggana Gunita pembedaan jenis layanan tersebut karena disitu juga terdapat perbedaan mengenai sejauh mana penyedia layanan dapat memiliki kontrol akses kepada data pelanggan dan pada umumnya pengguna layanan komputasi awan dari Biznet lebih banyak dikendalikan oleh pengguna masing-masing baik itu layanan individu maupun korporasi. Disini apabila terjadi kebocoran data ataupun penyalahgunaan yang disebabkan oleh kesalahan atau keteledoran dari pengguna maka hal tersebut menjadi tanggung jawab dari pengguna masing-masing

4.4.2 Lokasi Pusat Data Pelanggan Disimpan

Bila anda menggunakan penyedia komputasi awan, data anda ditransfer melalui internet ke dan dari satu atau lebih pusat data eksternal. Dalam hal ini data anda mungkin saja diproses olehpusat data di beberapa lokasi di seluruh dunia.Berbagai masalah hukum dapat muncul ketika data pelanggan berada di pusat daya penyedia awan di negara yang berbeda baik pelanggan atau klien pelanggan berada. Negara yang berbedadan dalam beberapa kasus bahkan negara bagian yang berbeda, provinsi atau kota, memiliki hukum yang berbeda yang berkaitan dengan data.

Tony Seno menyebutkan bahwa dalam layanan komputasi awan Microsoft terdapat 2 (dua) tipe lokasi server yaitu apabila layanan komputasi awan dengan *server* di Microsoft maka data tersebut akan tersebut di beberapa pusat data Microsoft di beberapa negara. Sedangkan apabila layanan komputasi awan dengan

server di mitra Microsoft maka data tersebut akan terletak di pusat data perusahaan-perusahaan mitra Microsoft itu.

Kebijakan pusat data yang hampir sama diadopsi oleh IBM Indonesia dimana pada saat ini IBM Indonesia memiliki dua model layanan komputasi awan yaitu *public cloud* dan *semi private cloud*. Untuk yang *public cloud*, pusat layanan terdekat ada di Singapura dan terhubung dengan 6 data center (pusat data) lain di seluruh dunia, sebagai bagian dari *redundancy concept* dan *disaster recovery*. Menurut Kurnia Wahyudi hal tersebut dilakukan selain kemudahan bagi pelanggan untuk mendapatkan layanan terdekat juga guna menurunkan isu/masalah *latency* (*slow response time*). Sedangkan untuk *semi private cloud*, IBM Indonesia sudah membangun pusat data di Indonesia, selain untuk menurunkan isu/masalah *latency* seperti tersebut di atas, juga berkaitan dengan regulasi pemerintah secara umum, bahwa data diupayakan untuk tidak keluar dari wilayah indonesia.

Sedangkan dalam layanan Biznet Cloud Computing sendiri seluruh data pelanggan disimpan pada Biznet MegaPOP Data Center di Jakarta pada saat ini. Kemudian pada tahun 2012 nanti Biznet akan menyediakan pusat data baru di daerah Cibubur bernama Biznet TeraPOP Cibubur dalam komplek Biznet Technovillage yang juga berfungsi sebagai *Disaster Recovery Center*. Semua pusat data Biznet berada di wilayah Indonesia

4.4.3 Tindakan Yang Dilakukan Oleh Penyedia Layanan Komputasi Awan Untuk Melindungi Data Pelanggan

Dalam layanan komputasi awan Microsoft, data pelanggan dilindungi menggunakan teknologi terkini yaitu virtualisasi, partisi,firewall, Information Rights Management,enkripsi dan desain Data Centeryang tersebar untuk meningkatkan availability. Menurut Tony Seno, untuk memastikan desain yang baik dan aman, Microsoft juga melakukan sertifikasi terhadap layanan awan Microsoft. Dan saat inilayanan awan Microsoft sudah mendapatkan sertifikasi FISMA, ISO 27001:2005, dan SAS 70type II.

Menurut Kurnia Wahyudi, IBM *sebagai technology and service provider* berupaya semaksimal mungkin memberikan layanan secara teknis dalam

melindungi data pelanggan, guna melindungi data pelanggan dari aspek keamanan (*security*), yang meliputi *Confidentiality*, *Integrity*, dan *Availbility* - sesuai tingkatan sekuriti yang pelanggan inginkan dalam bentuk *Service Level Agreement*. Termasuk di dalamnya hal-hal yang berhubungan dengan kebijakan, prosedur, standar layanan dan bantuan yang terkait dengan tingkatan sekuriti yang diinginkan oleh pelanggan

Kemudian dalam layanan komputasi awan Biznet, Anggana Gunita menjelaskan bahwa untuk melindungi data pelanggan, Biznet telah menuangkannya dalam *Service Level Agreement* dengan pengguna layanan dimana di dalamnya terdapat kewajiban dari pihak penyedia dan pengguna layanan komputasi awan. Dalam hal ini Biznet bertanggungjawab pada jaringan dan perangkat keras yang disediakan seperti menyediakan pihak keamanan pusat data 24 jam, menjaga pendinginan pusat data, dan menyediakan listrik beserta generator pendukung. Dan terkait dengan manajemen sekuriti data, dalam layanan ini pihak pengguna yang lebih dituntut untuk dapat mencegah terjadinya tindakan-tindakan yang mengganggu data mereka seperti *hacking*, *spamming, phising*, dan lain sebagainya, sedangkan Biznet lebih kearah preventif seperti menyediakan fitur-fitur *firewall*, update *antivirus*, dan update program atau *Virtual Machine* yang disediakan. Biznet menjamin atas ketersediaan layanan komputasi awan baik jaringan maupun perangkat keras hingga 99,8% dan pengguna layanan berhak mendapat penggantian hingga 30 (tiga puluh) persen dari jumlah total tagihan dalam sebulan jika Biznet tidak mencapai jaminan layanan yang dijanjikan pada *Service Level Agreement*.

4.4.4 Pertanggung jawaban dari Penyedia Layanan Komputasi Awan Apabila Data Pelanggan Tersebut Bocor atau Disalahgunakan

Dalam hal terjadi kebocoran atau penyalahgunaan data, Microsoft menghargai dan melindungi privasi data/informasi pelanggan dan tidak akan dibocorkan /disalahgunakan. Microsoft tidak akan mengungkapkan informasi pribadi Anda di luar Microsoft dan anak perusahaan yang dikendalikan dan

afiliasi tanpa persetujuan Anda[180]. Menurut Tony Seno, jika ada pelanggaran, maka Microsoft bisa terkena pelanggaran pasal privasi/keamanan data dalam UU ITE.

Sedangkan menurut Kurnia Wahyudi dari IBM Indonesia terkait dengan hal ini harus dilihat secara proporsional dan perlu investigasi yang mendalam perihal penyalahgunaan dan kebocoran. IBM selalu akan mengikuti peraturan dan undang-undang yang berlaku sesuai dengan kesepakatan yang dibuat dengan pelanggan, asalkan investigasi yang menyeluruh dan mendalam telah membuktikannya. Proporsionalitas untuk melihat di mana, oleh siapa, dan karena apa kebocoran dan penyalahgunaan terjadi, termasuk potensi terbesar hal itu terjadi. Beliau mencontohkan sebagai analogi perihal perlindungan data terhadap nomor telepon selular yang dimiliki oleh pelanggan baru (nomor yang baru dibuat), ternyata para provider telepon selular tak dapat melindungi nomor tersebut dari serangan SMS liar (baik penipuan maupun penawaran) yang diakibatkan beredarnya nomor tersebut oleh oknum yang tidak bertanggungjawab di internal provider (catatan: sang pemilik nomor baru belum pernah atau sempat mendistribusikan nomor nya yang baru kepada instansi yang memiliki potensi penyebaran yang tidak bertanggung jawab terjadi, seperti agen kartu kredit, asuransi, dan lain sebagainya)

Dan dalam layanan komputasi awan Biznet, Biznet tidak akan mengungkapkan informasi pengguna layanan kepada pihak ketiga tanpa persetujuan pengguna layanan. Biznet dapat bekerja sama dengan otoritas hukum dan / atau pihak ketiga dalam investigasi kejahatan apapun yang dicurigai atau diduga salah, termasuk pengungkapan informasi pengguna layanan, tetapi hanya jika Biznet diminta untuk melakukannya oleh hukum[181]. Sedangkan apabila terjadi kebocoran data atau penyalahgunaan data karena tindakan *hacking* maka Biznet dalam hal ini mencantumkannya dalam pasal *Force Majeure* dengan kewajiban untuk memberitahukan keadaan tersebut secepatnya kepada pengguna layanan.

[180]Microsoft Online Privacy Statement, <http://privacy.microsoft.com/en-us/fullnotice.mspx> Diakses pada 1 Januari 2012

[181]Biznet Networks Terms and Condition, <http://www.biznetnetworks.com/Id/?menu=terms_condition>, Diakses pada 1 Januari 2012

BAB 5
PENUTUP

5.1. **Kesimpulan**

Dari uraian bab-bab sebelumnya akhirnya penelitian ini sampai pada beberapa kesimpulan atas pembahasan permasalahan yang telah diteliti sebelumnya yaitu sebagai berikut :

1. Dari analisis perbandingan peraturan perundang-undangan yang mengatur mengenai perlindungan data pribadi di Uni Eropa dan Malaysia yang telah penulis lakukan ditemukan bahwa perumusan perlindungan data pribadi dalam UU ITE masih belum komprehensif. *EU Directive 95/46/EC* yang berlaku di Uni Eropa mendefinisikan secara jelas dan rinci pengaturan pihak-pihak yang terkait, memiliki prinsip-prinsip perlindungan data yang komprehensif hingga membatasi perpindahan data pribadi ke negara-negara yang dianggap tidak memiliki regulasi perlindungan data pribadi yang sepadan. Sedangkan pengaturan perlindungan data pribadi yang komprehensif dalam Malaysia *Personal Data Protection Act* lebih banyak ditujukan pada perlindungan data pribadi dalam transaksi komersial. *Malaysia Personal Data Protection Act* memiliki prinsip-prinsip perlindungan data pribadi, hak-hak baru bagi setiap orang terkait data pribadinya, pemuatan sanksi pidana, hingga pembentukan lembaga penasihat, pengawas dan penegakan hukum yang terkait dengan perlindungan data ini. Apabila kita membandingkan dengan pengaturan perlindungan data pribadi dalam UU ITE maka hanya ditemukan 2 (dua) prinsip perlindungan data yang diterapkan dalam pasal 26 UU ITE yaitu *Notice* atau pemberitahuan dan *Consent* atau persetujuan.

2. Indonesia belum memiliki Undang-undang yang khusus membahas mengenai privasi dan perlindungan data pribadi. Tetapi perlindungan privasi dan data pribadi dapat ditemukan di beberapa peraturan perundang-undangan. Khusus untuk perlindungan data pribadi yang secara spesifik berada di lingkup media elektronik terdapat dalam Pasal 26 Undang-

undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Untuk dapat mengembangkan layanan komputasi awan yang menghormati privasi dan melindungi data pribadi pengguna layanan maka diperlukan regulasi yang lebih komprehensif.

3. Terkait dengan tanggung jawab penyedia layanan komputasi awan terhadap data maupun data pribadi pengguna layanannya, penulis melihat bahwa terdapat beberapa perbedaan kebijakan teknis yang diterapkan untuk melindungi data tersebut. Dalam hal ini penyedia layanan awan telah menerapkan prinsip tanggung jawab sebelum suatu kejadian (*ex-ante liability*). Kemudian penulis dapat menarik kesimpulan dari narasumber-narasumber dari beberapa penyedia layanan komputasi awan dimana penyedia layanan komputasi awan menghormati, melindungi dan tidak akan mengungkapkan data pribadi pengguna layanan komputasi awan tanpa adanya persetujuan dari pengguna layanan. Hal ini tentu selaras dengan maksud dan tujuan dari rumusan Pasal 26 UU ITE. Sedangkan apabila terjadi malfungsi dari sistem komputasi awan yang mengakibatkan tidak terpenuhinya layanan maksimal kepada pengguna layanan, maka berdasarkan *Service Contract Agreement* dan *Service Level Agreement* penyedia layanan komputasi awan (dalam hal ini Biznet Networks) akan mengganti hingga 30 (tiga puluh) persen dari jumlah total tagihan dalam satu bulan. Di lain sisi apabila data pribadi pengguna layanan komputasi awan dicuri dan/atau dibobol oleh tindakan *hacking* dan/atau tindakan lain yang diluar kendali dari penyedia layanan maka penyedia layanan komputasi awan tidak bertanggungjawab atas kewajiban yang ditimbulkan dari gangguan tersebut dengan sebelumnya memberitahukan keadaan tersebut secepatnya kepada pelanggan

5.2. Saran

1. Perlu dibentuk pranata hukum yang secara khusus membahas dan mengatur mengenai perlindungan data pribadi agar perlindungan mengenai data pribadi dapat dilaksanakan dengan lebih menyeluruh.

Salah satunya dengan mendorong Pemerintah melalui Kementerian Komunikasi dan Informatika untuk mengesahkan Rancangan Peraturan Pemerintah (RPP) Penyelenggaraan Informasi dan Transaksi Elektronik (PITE).

2. Faktor keamanan dan privasi menjadi dua dari empat isu terpenting seputar implementasi komputasi awan di Indonesia, selain masalah keterbatasan akses Internet dan keberadaan data itu sendiri. Dari segi peraturan perundang-undangan, UU ITE belum cukup untuk mengakomodasi perlindungan data prbadi yang komprehensif. UU ITE tidak mengatur sejauh mana maksud dari "penggunaan data" dan tidak tersedianya alas hak secara hukum bagi pemilik data (subjek data) untuk mendapat akses ke data pribadinya dan melakukan perubahan terhadap data pribadinya yang berada di pengguna data. Dan sebelum dikeluarkannya undang-undang atau pengaturan yang lebih komprehensif mengenai perlindungan data pribadi maka para penyedia layanan komputasi awan sebaiknya mematuhi prinsip-prinsip perlindungan data pribadi untuk membangun hubungan kepercayaan kepada pengguna layanan komputasi awan yang lebih baik kedepannya.

DAFTAR REFERENSI

I. BUKU-BUKU

Barger, G.A. Lost in Cyberspace : Inventors, Computer Piracy and Printed Publications under section 102 (b) of the Patent Act of 1994. Detroit : Mercy L. Rev, 1994

Chee, Brian J.S dan Curtis Franklin Jr. Cloud Computing : Technologies and Strategies of the Ubiquitous Data Center. Gainesville : CRC Press, 2010

Dewi, Shinta. Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional. Bandung : Widya Padjajaran, 2009

Gutwirth et.al (ed). Computers, Privacy and Data Protection : an Element of Choice. London : Springer Books, 2011

Krutz, Ronald L dan Russel Dean Vines. Cloud Security : A Comprehensive Guide to Secure Cloud Computing. Indianapolis : Wiley Publishing Inc, 2010

Makarim, Edmon. Pengantar Hukum Telematika (Suatu Kompilasi Kajian). Jakarta : Raja Grafindo Persada, 2005

----------. Tanggung Jawab Hukum Penyelenggara Sistem Elektronik. Jakarta: Raja Grafindo Persada, 2010

Marrett, Paul. Information Law in Practice : 2nd Edition. Cornwall : MPG Books Ltd, 2002

Soekanto, Soerjono dan Sri Mamudji, Penelitian Hukum Normatif : Suatu Tinjauan Singkat. Ed.1. Cet. 10. Jakarta: Raja Grafindo Persada, 2007

II. PERATURAN PERUNDANG-UNDANGAN

Indonesia. Undang-Undang Dokumen Perusahaan. UU No. 8 Tahun 1997. LN No. 18 Tahun 1997. TLN No. 3674

----------. Undang-Undang Informasi dan Transaksi Elektronik. UU No. 11 Tahun 2008. LN No. 58 Tahun 2008. TLN No. 4843.

----------. Undang-Undang Kearsipan. UU No. 43 Tahun 2009. LN No. 152 Tahun 2009. TLN No.5071.

----------. Undang-Undang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. UU No. 10 tahun 1998. LN No. 182 Tahun 1998. TLN No. 3790.

----------. Undang-Undang Telekomunikasi. UU No. 36 Tahun 1999. LN No. 154 Tahun 1999. TLN No. 3881

III. JURNAL ILMIAH

Budhijanto, Danrivanto. "The Present and Future of Communication and Information Privacy in Indonesia" Jurnal Hukum Internasional Universitas Padjajaran Vol. 2, 2003

Chowdhury, Minamur. "Cloud Computing : Facts, Security and Legal Challenges" University of British Columbia Term Paper, 2009

Harbour, Laurel J, Ian D. Macdonald dan Eleni Gill. "Protection of Personal Data : The United Kingdom Perspective" Defense Counsel Journal, 2003

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

Kuo, Alex Mu-Hsing. "Opportunities and Challenges of Cloud Computing to Improve Health Care Services" Journal of Medical Internet Research, 2011

Kyer, C. Ian dan Gabriel M.A. Stern. "Where in the World is My Data? Jurisdictional Issues with Cloud Computing" Fasken Martineau, 2011

Leong, Foong Cheng dan Halina Jael Abu Bakar. "Personal Data Protection Act 2010" Legal Herald July-September Edition, 2010

Mell, Peter dan Timothy Grance, "The NIST Definition of Cloud Computing" National Institute of Standards and Technology, United States Department of Commerce, 2011

Ryan, Michael W dan Christoper M. Leoffler, "Insights into Cloud Computing" Intellectual Property and Technology Law Journal Vol 22 Number 11, 2010

Shilling, Cameron G., "Privacy and Data Security : New Challenges of The Digital Age". New Hampshire Bar Journal, 2011

Wyld, David C. "The Cloudy Future of Government IT : Cloud Computing and The Public Sector Around The World" International Journal of Web & Semantic Technology (IJWesT), Vol 1, 2010

IV. MAKALAH / HASIL PENELITIAN

Gwijangge, Diaz. "Peran TIK Dalam Pembangunan Karakter Bangsa." Makalah Disampaikan dalam Workshop: "Pemanfaatan Jejaring E-Pendidikan" yang diselenggarakan Pusat Teknologi Informasi dan Komunikasi Pendidikan Kementerian Pendidikan Nasional, Sulawesi Selatan, 14 Juni 2011

Herwina Anggeriana, dkk. "Cloud Computing". Makalah dapat diakses di < http://lutung.lib.ums.ac.id/dokumen/ebooks/Komputer/Cloud%20Computing/Cloud-Computing.pdf >

Ian Mitchell, dkk. "The Fujitsu White Book of Cloud Computing : The Definitive Guide to a Business Technology Revolution". Makalah dapat diakses di <https://sp.ts.fujitsu.com/dmsp/docs/wp-cloud-adoption1.pdf>

Indrajit, Richardus Eko. "Fenomena Kebocoran Data : Mencari Sumber Penyebab dan Akar Permasalahannya." Makalah dapat diakses di < http://www.idsirtii.or.id/content/files/IDSIRTII-Artikel309-FenomenaKebocoranData.pdf >

Purwanto. "Penelitian Tentang Perlindungan Hukum Data Digital". Jakarta : Badan Pembinaan Hukum Nasional, 2007

Setiawan, Deris. "Mengenal Cloud Computing". Makalah dapat diakses di <http://deris.unsri.ac.id/materi/jarkom/mengenal_cloudcomputing.pdf>

Stratford, Slemmons Jean dan Juri Stratford. "Data Protection and Privacy in the United States and Europe". Makalah dapat diakses di <www.iassistdata.org/downloads/iqvol223stratford.pdf>

Wardiana, Wawan. "Perkembangan Teknologi Informasi di Indonesia." Makalah disampaikan dalam Seminar dan Pameran Teknologi Informasi 2002, Fakultas Teknik Universitas Komputer Indonesia (UNIKOM) Jurusan Teknik Informatika, Bandung, 9 Juli 2002

West, Darrel M. "Saving Money Through Cloud Computing". Makalah dapat diakses di <http://www.brookings.edu/~/media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf>

Yusmansyah, Efrizal Fikri. "Proteksi Internet Privacy dengan Protokol P3P". Makalah dapat diakses di <http://www.cert.or.id/~budi/courses/ec7010/2004-2005/fikri-report/report-fikri-23203089.doc>

V. MAJALAH

Nistanto, Reska K. "Membidik UKM dengan Cloud" Bloomberg Businessweek (14-20 April 2011), hlm. 16

VI. INTERNET

"Kampanyekan Cloud Dengan Solusi Satu Kotak." <http://tekno.kompas.com/read/2011/09/12/2144062/Kampanyekan.Cloud.dengan.Solusi.Satu.Kotak> Diakses pada 13 September 2011

"Cisco: Pendapatan dari Public Cloud Computing Dunia diperkirakan US$44 M di 2013" <http://www.wartaekonomi.co.id/berita-115429668-cisco-pendapatan-dari-public-cloud-computing-dunia-diperkirakan-us44-m-di-2013.html.>Diakses pada 22 Agustus 2011

"Pasar Komputasi Awan Tumbuh 53,4%". < http://www.bisnis.com/articles/pasar-komputasi-awan-tumbuh-53-4-percent>. Diakses pada 10 Oktober 2011

"Top 20 Countries With The Highest Number of Internet Users", <http://www.internetworldstats.com/top20.htm> Diakses pada 20 Agustus 2011

"International Cloud Computing Trend : Indonesia", <http://www.cloudbusinessreview.com/2011/08/15/international-cloud-computing-trend-indonesia.html> Diakses pada 20 Agustus 2011

"Pasar Cloud Computing di Indonesia Terbuka Lebar". <http://www.kabarbisnis.com/read/2818810 >. Diakses pada 20 Agustus 2011

"Indonesia Sudah Siap Sambut Komputasi Awan." <http://news.okezone.com/read/2011/05/25/324/460984/indonesia-sudah-siap-sambut-komputasi-awan.> Diakses pada 15 Agustus 2011

Perusahaan Masih Ragu Adopsi Cloud Computing. <http://techno.okezone.com/read/2011/05/03/324/452885/perusahaan-masih-ragu-adopsi-cloud-computing>. Diakses pada 21 Agustus 2011

"A Corporate PC Trends and Buyer Behaviour Survey" <http://www.lenovo.com/news/za/en/2011/03/survey.html> Diakses pada 21 Agustus 2011

Pravin Kothari. Building Trust In The Cloud. <http://www.siliconindia.com/magazine_articles/Building_Trust_in_the_Cloud-UNPN806818863.html> . Diakses pada 13 September 2011

The Legal Issues Around Cloud Computing. <http://www.labnol.org/internet/cloud-computing-legal-issues/14120> Diakses pada 22 Agustus 2011

Annual Report Form 10-K Google Inc and United States Securities and Exchange Comission. <http://investor.google.com/documents/20101231_google_10K.html> Comission file number 000-50726. Diakses pada 27 Agustus 2011. Hlm 52

Jaringan Sony Dibobol Lagi, Jutaan Data Dicuri. <http://www.tempo.co/hg/it/2011/06/03/brk,20110603-338366,id.html> Diakses pada 13 September 2011

Pradiptya, Dionysisus Damas. "Pengaturan Perlindungan Data di Indonesia," Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia < http://indocyberlaw.org/?p=313> Diakses pada 1 November 2011

EU Cloud Data Can Be Secretly Accessed by US Authorities. <http://www.theregister.co.uk/2011/07/04/eu_customer_cloud_data_may_be_handed_over_by_microsoft/> Diakses pada 16 Oktober 2011

New Data Privacy Law in Malaysia.< http://www.bakermckenzie.com/RRSingaporeNewDataPrivacyLawAug10/> Diakses pada 9 Oktober 2011

Abu Bakar Munir, "The Malaysian Personal Data Protection Bill", <http://profabm.blogspot.com/2009/12/malaysian-personal-data-protection-bill.html> Diakses pada 24 Oktober 2011

Pendapatan Cloud Computing di Indonesia Tumbuh 48% hingga 2014, <http://www.indonesiafinancetoday.com/read/16131/Pendapatan-Cloud-Computing-di-Indonesia-Tumbuh-48-hingga-2014> Diakses pada 16 November 2011

Komputasi Awan Masih Di Awang-Awang. < http://tekno.kompas.com/read/2011/07/04/03225759/Komputasi.Awan.Masih.di.Awang-awang > Diakses pada 30 November 2011

Era Komputasi Awan < http://www.bunyu-online.com/2009/05/era-komputasi-awan.html > Diakses pada 14 November 2011

Falahuddin, Mochamad James. "Lebih Jauh Mengenal Komputasi Awan" < http://www.detikinet.com/read/2010/02/24/084138/1305595/328/lebih-jauh-mengenal-komputasi-awan > Diakses pada 14 November 2011

Cloud Computing, < http://www.syntheticlepathy.net/information-and-communication-technology/cloud-computing/> Diakses pada 14 November 2011

Cloud Computing for Business Cuts Cost by 50 Percent, < http://www.cloudbusinessreview.com/2010/11/20/cloud-computing-for-business-cuts-costs-by-50-percent.html > Diakses pada 30 November 2011

ISACA, "Cloud Computing : Business Benefits With Security, Governance and Assurance Perspective" < http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_%26_Governance-ISACA.pdf > Diakses pada 18 November 2011

Hartono, Tony Seno. "Komputasi Awan dan Segala Aspeknya", < http://www.detikinet.com/read/2011/10/26/093855/1752688/328/komputasi-awan-dan-segala-aspeknya > Diakses pada 30 November 2011

Shannon, David J. " Storage of Trade Secrets in Cloud Computing", < http://www.databreachlegalwatch.com/2011/05/storage-of-trade-secrets-in-cloud-computing/ > Diakses pada 11 Desember 2011

Stephen Withers, "Singapore Regulator Casts Doubt on Banking Clouds",< http://www.itnews.com.au/News/235977,singapore-regulator-casts-doubt-on-banking-clouds.aspx > Diakses pada 12 Desember 2011

"77 Juta Data Konsumen Sony PlayStation Dibobol", < http://fokus.vivanews.com/news/read/216981-77juta-data-pengguna-sony-playstation-dibobol > Diakses pada 6 Desember 2011

"Ribuan Data Penting Konsumen Sony Bobol", < http://fokus.vivanews.com/news/read/218210-lagi--12-ribu-data-konsumen-sony-bobol > Diakses pada 6 Desember 2011

Mary Helen Miller, "Sony Data Breach Could Be Most Expensive Ever", < http://www.csmonitor.com/Business/2011/0503/Sony-data-breach-could-be-most-expensive-ever > Diakses pada 6 Desember 2011

Reitinger, Phillip. "An Important Message From Sony's Chief Information Security Officer", < http://blog.eu.playstation.com/2011/10/12/an-important-message-from-sonys-chief-information-security-officer/> Diakses pada 7 Desember 2011

Newman, Jared. "Google Issues Patch to Plug Android Data Leaks", < http://www.pcworld.com/article/228146/google_issues_patch_to_plug_android_data_leaks.html > Diakses pada 6 Desember 2011

----------. "Researchers Discover Android Data Leaks : What You Need to Know, < http://www.pcworld.com/article/228045/researchers_discover_android_data_leaks_what_you_need_to_know.html > Diakses pada 6 Desember 2011

Suryadi, Ardhi. "1,3 Juta Data Pengguna SEGA Dicuri", < http://www.detikinet.com/read/2011/06/20/092356/1663626/323/13-juta-data-pengguna-sega-dicuri/ > Diakses pada 6 Desember 2011

"Peretas Bobol Data Pengguna Perusahaan Permainan SEGA", < http://www.pikiran-rakyat.com/node/149206 > Diakses pada 6 Desember 2011

"Data 200 Ribu Nasabah Citibank AS Dicuri", <http://bisnis.vivanews.com/news/read/225917-data-200-ribu-nasabah-citibank-dicuri-di-as > Diakses pada 7 Desember 2011

Microsoft Online Privacy Statement, <http://privacy.microsoft.com/en-us/fullnotice.mspx> Diakses pada 1 Januari 2012

Biznet Networks Terms and Condition, <http://www.biznetnetworks.com/Id/?menu=terms_condition>, Diakses pada 1 Januari 2012