TANGGUNG JAWAB PENYEDIA LAYANAN KOMPUTASI AWAN TERHADAP PERLINDUNGAN DATA PRIBADI PENGGUNA LAYANAN KOMPUTASI AWAN (BERDASARKAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK NOMOR 11 TAHUN 2008)

Sulaiman[1]

[1]Dosen Fakultas Hukum, Universitas Tarakan Kalimantan Utara, Universitas Borneo Tarakan, Jl. Pantai Amai No 1. Tarakan, Indonesia.

Penyesuaian Pengarang E-mail: sulaiman.hukum@gmail.com

No Hp: 081254295229

ABSTRAK

Dalam perkembangan teknologi informasi, yang memunculkan berbagai macam sarana Informasi dan komunikasi serta suatu layanan penyimpanan data yang berbasis internet. Sehingga kebanyakan masyarakat yang menggunakan media elektronik dan menyimpan data pribadi dilayanan komputasi awan (*Cloud Computing)* sebagai alat penyimpanan data serta informasi yang berpotensi terjadinya penyalahgunaan data pribadi. Dalam penelitian ini penulis memaparkan mengenai tanggung jawab penyedia layanan Komputasi Awan atas data Pribadi pengguna layanan, hal ini terkait mengenai penerapan pasal perlindungan data pribadi yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dikaitkan dengan praktik layanan komputasi awan yang saat ini sedang berkembang pesat. Penelitian ini bertujuan untuk menganalisis serta menjelaskan pokok-pokok permasalahan yang ingin diungkap berdasarkan rumusan masalah yaitu makna hukum perlindungan data pribadi yang terdapat dalam Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan konsep hukum agar tercipta perlindungan hukum terhadap data pribadi penguna layanan dan tanggung jawab dari penyedia layanan komputasi awan terhadap data pribadi pengguna layanan.

Kata kunci: komputasi awan, perlindungan hukum data pribadi, tanggung jawab

PENDAHULUAN

Latar Belakang Masalah

Perkembangan teknologi informasi salah satunya membawa pengaruh terhadap semakin konvergennya sistem komputasi *(computing system)* dan sistem komunikasi yang mendorong terintergerasi kedua sistem tersebut pada jarak jauh *(telecommunication system).* Cepatnya perkembangan teknologi informasi dan diterimanya internet secara luas sebagai infrastruktur alternatif modern, tidak berarti bahwa eksistensi keduanya tidak memunculkan permasalahan-permasalahan, baik yang bersifat teknis maupun yang bersifat yuridis. Perkembangan teknologi informasi

yang berkembang cepat sangat jauh perbedaanya dengan masa awal kehadirannya. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung secara cepat dengan *signifikan.*

Inovasi yang ditawarkan melalui *cloud computing* ini sangat berpotensi untuk mengembangkankegiatan perekonomian, baik olehorganisasi kecil maupun organisasi besar. Tanpa harus mengeluarkan biaya banyak dalam hal teknologi, kegiatan ekonomi suatu perusahaan dapat berjalan efektif dan efisien. Hal tersebut itulah yangsangat diperlukan oleh organisasi-organisasi kecilyang akan memulai usaha. Di samping itu penggunaan teknologi sudah menjadi keharusan bagi para pelaku bisnis.

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*.[1] Pada tahun 2015 tersebut, trafik internet bisa mencapai hingga ukuran *zetabyte* atau miliar-miliar juta *bytes*.[2] 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*. 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.

Perlindungan data begitu penting antara lain adalah mengenai data pertahanan keamanan negara dan data pasar modal. Hal tersebut dapat dilihat dari 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, jenis dan jumlah persenjataan. Di dalam kegiatan pasar modal, data merupakan sesuatu yang vital karena itu perlindungan data dalam pasar modal begitu sangat signifikan terkait dengan penggunaan data termasuk juga infrastukturnya.

Berdasarkan banyaknya isu hukum yang melingkupi teknologi yang terbilang baru ini, maka penulis tertarik untuk penelitian dan menulis Tesis dengan judul "Tanggung Jawab Penyedia Layanan Komputasi Awan Terhadap Perlindungan Data

[1] "Kampanyekan *Cloud* Dengan Solusi Satu Kotak". <http://tekno.kompas.com/read /2011/09/12/2144062/Kampanyekan. *Cloud*. dengan. Solusi. Satu. Kotak> Diakses pada 19 Oktober 2014

[2] *Ibid.*

Pribadi Pengguna Layanan Komputasi Awan (Berdasarkan Undang-Undang Nomor 11 Tahun 2008).” Untuk mencoba memberikan jawaban terkait jaminan hukum dan melindungi kepentingan pengguna baik personal maupun perusahaan yang menggunakan jasa fasilitas penyedia layanan Komputasi Awan terhadap data pribadi mereka di Indonesia.

Rumusan Masalah

Berdasarkan uraian dan batasan masalah di atas, penulis akan mengangkat permasalahan guna dibahas dalam penulisan tesis ini, yaitu: Bagaimana tanggung jawab penyedia layanan komputasi awan terhadap perlindungan data pribadi pengguna layanan komputasi awan?

HASIL PENELITIAN DAN PEMBAHASAN

Tanggung jawab hukum disini berpedoman pada tanggung jawab sebelum terjadinya suatu kejadian, dan tanggung jawab setelah kejadian.Tanggung jawab sebelum sesuatu kejadian adalah tanggung jawab untuk mematuhi semua undang-undang dan/atau regulasi mengenai Teknologi Informasi (TI) dalam rangka memberi sesuatu yang layak kepada publik (penerapan prinsip tata kelola yang baik terhadap penyelenggaraan sesuatu). Sementara tanggung jawab setelah kejadian adalah tanggung jawab untuk memulihkan keadaan bagi yang dirugikan kepada keadaan yang semula.[3]

Tanggung jawab hukum dalam penyelenggaraan sistem elektronik ditentukan berdasarkan undang-undang yang disebut juga Perbuatan Melawan Hukum (PMH). Perbuatan melawan hukum lahir karena adanya prinsip bahwa barang siapa melakukan perbuatan yang membawa kerugian kepada oranglain mewajibkan orang yang salah karena salahnya mengganti kerugiantersebut (Pasal 1365 KUHPer). Sesuai dengan ketentuan Pasal 1365 Kitab Undang-Undang Hukum Perdata, suatu perbuatan melawan hukum (PMH) harus mengandung unsur-unsur sebagai berikut;(1) ada suatu perbuatan, (2) perbuatan itu melawan hukum, (3) ada kesalahan dari pelaku, (4) ada kerugian korban, (5) ada hubungan kausal antara perbuatan dan kerugian.

[3] Indroharto, *Usaha Memahami Undang-Undang tentang Peradilan Tata Usaha Negara: Buku I Beberapa Pengertian Dasar Hukum Tata Usaha Negara*. Jakarta: Sinar Harapan, 2000, hal. 39 dikutip dari Edmon Makarim, *Tanggung Jawab Penyelenggara Terhadap Tata Kelola Yang Baik Dalam Penyelenggaraan Sistem Elektronik* (*Good Electronic Governance),* Jakarta: Ringkasan Desertasi, FHUI, 2009, hal. 79

Dalam penyelenggaraan sistem elektronik pengadaan tanggung jawab dibedakan dari sisi prosedural atau administratif (*business process*) dan dari sisi teknis. Dari sisi prosedural ditentukan berdasarkan proses administrasiyang seharusnya dilakukan, sedangkan dari sisi teknis ditentukan berdasarkantata kelola teknologi yang baik dan tepat. Dahulu, 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 negatif bagi kepentingan perlindungan konsumen.[4] Penerapan tanggung jawab penyedia layanan komputasi awan di sini bisa mengacu pada teori-teori tanggung jawab penyelenggara sistem elektronik.

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*.

Tanggung jawab sebelum suatu kejadian (*ex-ante liability*) adalah tanggung jawab untuk mematuhi semua undang-undang dan/atau regulasi administrasi Negara dalam rangka memberikan suatu yang layak kepada publik.[5] 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.[6]

Ada beberapa masalah hukum yang terkait dengan komputasi awan (*cloud computing)* itu sendiri. Namun dalam hal ini ada 2 (empat) permasalahan terkait dengan tanggungjawab penyedia layanan komputasi awan yang ingin diketahui yaitu:

1. Tindakan yang dilakukan oleh penyedia layanan komputasi awan untuk melindungi data pelanggan.

[4] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Raja Grafindo Persada, 2010, hal. 225
[5] *Ibid*, hal.160
[6] Ibid.

2. Pertanggung jawaban dari penyedia layanan komputasi awan apabila data pelanggan tersebut bocor atau disalahgunakan.

Penjabaran masing-masingnya akan dijabarkan sebagai berikut:

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

Layanan komputasi awan Telkom Indonesia atau yang dikenal dengan *Telkom Cloud*nya, data pelanggan dilindungi menggunakan teknologi terkini yaitu *virtualisasi, partisi, firewall, Information Rights Management, enkripsi* dan *desain* Data *Center* yang tersebar untuk meningkatkan *availability*. Sama halnya dengan *Microsoft,* Menurut Tony Seno, untuk memastikan desain yang baik dan aman, Microsoft juga melakukan sertifikasi terhadap layanan awan Microsoft. Saat ini layanan awan Microsoft sudah mendapatkan sertifikasi FISMA, ISO 27001: 2005, dan SAS 70 type 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.

Layanan komputasi awan Biznet, Anggana Gunita juga 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.

Terkait dengan manajemen sekuriti data, dalam layanan ini pihak pengguna yang lebih dituntut untuk dapat mencegah terjadinya tindakantindakan 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*.

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

Dalam hal ini, terjadi kebocoran atau penyalahgunaan data, Telkom menghargai dan melindungi privasi data/informasi pelanggan dan tidak akan dibocorkan /disalahgunakan. Namun pada dasarnya kebocoran data ataupu penyalahgunaan data memang sulit untuk dipungkari dikarenakan akibat musibah/bencana yang diakibatkan oleh manusia itu sendiri yang disebut Haeker (pembobol Pertanggung jawaban dari penyedia layanan itu sendiri yang merupakan suatu kewajiaban maka dari itu Telkom selalu meningkatkan keamanan data, sehingga kebocoran dan penyalahgunaan data yang disimpan bisa diminilisir.

Microsoft tidak akan mengungkapkan informasi pribadi Anda di luar *Microsoft* dan anak perusahaan yang dikendalikan dan *afiliasi* tanpa persetujuan Anda.[7] Menurut Tony Seno, apabila ada pelanggaran, maka Microsoft dapat dikenakan pelanggaran pasal privasi/keamanan data dalam Undang-Undang 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 dimana, oleh siapa, dan karena apa kebocoran dan penyalahgunaan terjadi, termasuk potensi terbesar hal itu terjadi.

[7] Microsoft Online Privacy Statement, <http://privacy.microsoft.com/enus/ fullnotice.mspx> Diakses pada 1 Januari 2012

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 nomornya yang baru kepada instansi yang memiliki potensi penyebaran yang tidak bertanggung jawab terjadi, seperti agen kartu kredit, asuransi, dan lain sebagainya).

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.[8] 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.

Dari uraian di atas maka dapat disimpulkan bahwa, Tanggung Jawab Penyedia Layanan Komputasi Awan Terhadap Data Pengguna adalah sebagai berikut :

1. 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.
2. Dalam hal ini penyedia layanan awan telah menerapkan prinsip tanggung jawab sebelum suatu kejadian (*ex-ante liability*).
3. 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.

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

4. Data pribadi pengguna layanan komputasi awan apabila 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.

KESIMPULAN DAN SARAN

Kesimpulan

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

1. Tindakan yang dilakukan

   Berfungsi untuk 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. 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.
2. Tanggung Jawab Penyedia Layanan Komputasi Awan Terhadap Data Pengguna adalah sebagai berikut :
   a. 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.
   b. Dalam hal ini penyedia layanan awan telah menerapkan prinsip tanggung jawab sebelum suatu kejadian (*ex-ante liability*).
   c. Nara sumber-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.

d. Data pribadi pengguna layanan komputasi awan apabila 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.

Saran

Faktor keamanan dan privasi menjadi dua dari empat isu terpenting seputar implementasi komputasi awan di Indonesia, selain masalahketerbatasan akses Internet dan keberadaan data itu sendiri. Dari segi peraturan perundang-undangan, Undang-Undang ITE belum cukup untuk mengakomodasi perlindungan data pribadi yang komprehensif. Undang-Undang 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.

Dalam hal ini, 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. Selain itu perlu dibentuk lembaga atau satuan tugas khusus untuk perlindungan data pribadi dan privasi antar beberapa instansi/lembaga terkait mengingat data pribadi pelanggan atau konsumen yang terkait dengan beberapa bidang, diantaranya telekomunikasi, perbankan, properti, tindak pidana penipuan, dan lainnya.

DAFTAR PUSTAKA

Buku, Jurnal dan Makalah

Edmon Makarim, Tanggung Jawab Penyelenggara Terhadap Tata Kelola Yang Baik Dalam Penyelenggaraan Sistem Elektronik (*Good Electronic Governance*), Jakarta: Ringkasan Desertasi, FHUI, 2009, hal. 79

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

Website

Biznet Networks Termsand Condition, <http://www.biznetnetworks.com/Id/?

menu=terms_condition>, Diakses pada 1Januari 2012

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