PERLINDUNGAN HUKUM ATAS DATA PENGGUNA OLEH PENYEDIA LAYANAN *CLOUD COMPUTING* DITINJAU DARI UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Arum Fatmawati
S1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya arumfatma622@gmail.com

Budi Hermono, S.H., M.H.
S1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya budihermono@unesa.ac.id

Abstrak

Skripsi ini membahas tentang perlindungan data berupa dokumen elektronik yang dikaitkan dengan kegiatan pemanfaatan *cloud computing* ditinjau dari Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Pesatnya penggunaan layanan *cloud computing* di Indonesia ini mendorong peningkatan jumlah pengguna yang menyimpan data di server layanan *cloud computing*. Sebagai sebuah layanan yang terbilang baru pemanfaatannya di Indonesia, menyimpan data di *cloud* ini menimbulkan kekhawatiran bagi pengguna terutama mengenai isu keamanan dan kerahasiaan data. Potensi kebocoran data yang mungkin dialami oleh penyedia layanan *cloud computing* dapat menimbulkan kerugian bagi pengguna layanan *cloud computing*. Penelitian ini merupakan penelitian normatif. Pendekatan penelitian yang digunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Jenis bahan hukum terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan nonhukum. Teknik pengumpulan bahan hukum yang digunakan adalah studi kepustakaan yang kemudian diolah dengan menggunakan sistem seleksi bahan hukum dalam teknik pengolahan bahan hukum. Hasil penelitian menunjukkan bahwa UU ITE belum mengatur mengenai perlindungan data khususnya berupa dokumen elektronik dalam kegiatan pemanfaatan teknologi *cloud computing*. Ketentuan hukum mengenai kewajiban perlindungan data serta tanggung jawab penyedia layanan *cloud computing* tidak diatur secara eksplisit dalam undang-undang tersebut sehingga timbul ketidakpastian hukum bagi pengguna layanan *cloud computing*. Pasal 26 UU ITE secara khusus mengatur mengenai perlindungan data pribadi yang mana hal tersebut tidak mencakup perlindungan dokumen elektronik pada pemanfaatan *cloud computing*. Penelitian ini membahas mengenai konsep umum perlindungan data, peraturan perundang-undangan yang mengatur tentang perlindungan data di Indonesia, prinsip-prinsip perlindungan data oleh penyedia layanan *cloud computing*, analisis pasal-pasal dalam UU ITE mengenai perlindungan data dan tanggung jawab dari penyedia layanan *cloud computing* terhadap data pengguna layanannya.
Kata kunci: *cloud computing*, perlindungan data, tanggung jawab hukum.

Abstract

This research discusses the data protection of electronic documents associated with the use of *cloud computing* in terms of Law Number 11 Year 2008 Concerning Information and Electronic Transactions (IET Act). The increasing use of *cloud computing* services boosts the number of users who store their data in the *server* of *cloud computing* services. As a relatively new service in Indonesia, storing data up in the cloud is raising concerns for users, especially regarding issues of security and data privacy. The potential of data leakage may be experienced by the service provider of *cloud computing* may result in losses for the users of *cloud computing* services. This research is normative. The research approach used is legislation approach and conceptual approaches. The type of legal materials consists of primary, secondary and non legal materials. The technique of legal materials collecting used in this research are literature studies then processed using a selection system for legal materials in processing techniques. The results showed that IET Act has not regulated the data protection, particularly electronic documents in activity of utilization of *cloud computing* technology. The legal provisions concerning data protection obligations and responsibilities of the service provider of *cloud computing* are not explicitly regulated in the legislation which resulting in legal uncertainty for users of *cloud computing* services. This research discusses the general concept of data protection, laws and regulations legislation governing data protection in Indonesia, the principles of data protection by providers of *cloud computing* services, the analysis of the articles of the IET ACT towards the data

protection and the responsibility of the *cloud computing* service provider to user data services.
Keywords: cloud computing, data protection, legal liability.

PENDAHULUAN

Teknologi informasi dan komunikasi mengalami perkembangan yang begitu pesat. Perkembangan tersebut memberikan manfaat yang besar bagi aktivitas manusia dalam menghemat waktu dan biaya, mempermudah kegiatan manusia dalam distribusi informasi serta berkomunikasi. Kehadiran teknologi *cloud computing* saat ini, membantu memudahkan berbagai kegiatan manusia. Perkembangan *cloud computing* pada saat ini merupakan bagian integral dalam perencanaan strategis teknologi informasi suatu organisasi atau perusahaan.[1]

Cloud computing disebut sebagai teknologi internet baru yang menyediakan infrastruktur fleksibel, efisien dan bermacam-macam aplikasi untuk bisnis.[2] Berdasarkan sebuah artikel *Communications World Weekly* yang merupakan majalah teknologi terkemuka di Cina menyebutkan bahwa *cloud computing* adalah generasi keempat revolusi di bidang teknologi informasi setelah penemuan *mainframe*, komputer, dan internet.[3]

Cloud computing merupakan gabungan pemanfaatan teknologi komputer dalam suatu jaringan dengan pengembangan berbasis internet yang mempunyai fungsi untuk menjalankan program atau aplikasi di mana kapabilitas terkait teknologi informasi disajikan sebagai suatu layanan *(as a service)*. Keuntungan dan manfaat penggunaan *cloud computing* mendorong minat masyarakat untuk menggunakan teknologi ini. Menurut studi yang dilakukan Cloudswave Research, pertumbuhan *cloud computing* secara global hingga tahun 2020 diperkirakan mencapai 30% dengan pendapatan sebesar US$ 270 milyar.[4] Tren penggunaan *cloud computing* menjadi global dan mulai diadopsi oleh negara Indonesia. Dalam lima tahun terakhir, teknologi *cloud computing* di Indonesia mengalami pertumbuhan sebesar 48% yang mana lebih tinggi dari pertumbuhan global tahunan yaitu sebesar 30%. Bahkan Indonesia menempati peringkat 11 dalam tingkat pertumbuhan pengguna *cloud computing* di wilayah Asia-Pasifik.

Mengikuti peningkatan permintaan *cloud computing* yang cukup tinggi tersebut, perusahaan asing maupun lokal mulai menawarkan solusi *cloud computing* untuk badan usaha dalam negeri.[5] Beberapa perusahaan dalam negeri, yaitu PT Telkom yang meluncurkan Telkom Cloud secara resmi pada tahun 2010[6], PT Infinys System Indonesia dengan infinyscloud pada tahun 2010[7], PT Cyberindo Mega Persada dengan CBNCloud pada pertengahan 2011[8], PT Biznet Networks dengan biznetgiocloud dan beberapa penyedia layanan *cloud computing* lainnya.[9]

Beberapa tahun terakhir, terdapat banyak isu kebocoran data yang telah dialami oleh para penyedia layanan *cloud computing*,*s* salah satu di antaranya adalah DropBox. DropBox merupakan media penyimpanan *online* yang dioperasikan oleh Dropbox Inc di Amerika Serikat. Kebocoran data yang dialami DropBox terjadi pada tahun 2012.[10] Sebanyak 6,937,081 akun pengguna DropBox lengkap dengan *username* dan *password* diambil alih sekelompok *hacker* akibat peretasan pada *server* Dropbox.[11]

Beberapa peristiwa kebocoran data dari *cloud* menyebabkan pengguna merasa sangat khawatir akan keamanan datanya. Oleh karena itu, diperlukan upaya pengamanan terhadap data pengguna dalam layanan *cloud computing*. Penjelasan umum Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) menyebutkan bahwa untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Dalam pemanfaatan teknologi tersebut, penyelenggaraan layanan *cloud computing* di Indonesia diakomodasi oleh UU ITE Pasal 26 UU ITE yang

[1] Berkah I Santoso. 2012. *E-book: Cloud Computing Strategi TI Modern*,(http://www.cloudindonesia.or.id/wp-content/uploads/2012/07/E-Book-Cloud-Computing-dan-Strategi-TI-Modern1.pdf, diunduh 6 Maret 2016) hal 3.

[2] Ibid.

[3] Red Akrim. 2012. *Cloud Computing: the 4th IT Industrial Revolution*,(https://www.cloudswave.com/blog/cloud-computing-the-4th-it-industrial-revolution/, diakses 6 Maret 2016)

[4] Red Akrim. 2015. *The Growth of Cloud Computing in Emerging Asian Market*, (https://www.cloudswave.com/blog/the-growth-of-cloud-computing-in-emerging-asian-market/, diakses 4 Februari 2016)

[5] *Ibid*

[6] Telkom Indonesia. 2010. *Telkom Cloud* (http://old.telkomcloud.com/News/5, diakses 24 Maret 2016).

[7] Infinys System Indonesia. 2014. *Infinys The True Cloud Company* (http://www.isi.co.id/, diakses 24 Maret 2016).

[8] Cyberindo Mega Persada. 2011. *CBN Cloud.* (http://wp.cbncloud.co.id/about-us/, diakses 24 Maret 2016).

[9] Biznet Gio Nusantara. 2014. *BiznetGioCloud.* (http://www.biznetgiocloud.com/about.php, diakses 24 Maret 2016).

[10] Insaf Albert Tarigan. 2014. *Ganti Password, 7 Juta Akun Dropbox Diretas*, (http://teknologi.metrotvnews.com/read/2014/10/15/305077/ganti-password-7-juta-akun-dropbox-diretas, diakses 4 Februari 2016)

[11] *Ibid.*

menyatakan, "Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media eletronik yang menyangkut data privasi seseorang harus dilakukan atas persetujuan orang yang bersangkutan." Meskipun telah terdapat pengakuan atas perlindungan data dalam informasi dan transaksi elektronik dalam UU ITE sebagaimana dalam Pasal 26 beserta penjelasannya, tetapi kewajiban perlindungan serta upaya perlindungan yang seharusnya dilakukan oleh pihak-pihak terkait seperti penyelenggara sistem elektronik ataupun pemerintah belum terdapat dalam UU ITE.[12] Selain itu, ketentuan dalam pasal tersebut tidak mencakup perlindungan data berupa dokumen elektronik yang umumnya disimpan pengguna dalam layanan *cloud computing.* Pada penelitian ini, penulis memfokuskan penelitian pada perlindungan data berupa dokumen elektronik.

Berdasarkan latar belakang di atas, permasalahan hukum yang diteliti adalah (1) Bagaimana seharusnya kewajiban melindungi data pengguna layanan *cloud computing* oleh penyedia layanan *cloud computing* dalam UU ITE?; dan (2) Bagaimana tanggung jawab hukum penyedia layanan *cloud computing* terhadap perlindungan data pengguna layanan *cloud computing* ditinjau dari UU ITE?

Tujuan penelitian ini adalah (1) menganalisis kewajiban perlindungan data pengguna layanan *cloud computing* oleh penyedia layanan *cloud computing* ditinjau dari UU ITE; (2) menganalisis tanggung jawab hukum penyedia layanan *cloud computing* terhadap perlindungan data pengguna layanan *cloud computing* ditinjau dari UU ITE.

METODE

Penelitian ini merupakan jenis penelitian hukum normatif. Penelitian hukum normatif merupakan penelitian hukum yang dilakukan berdasarkan norma dan kaidah peraturan perundang-undangan.[13] Di samping sumber-sumber penelitian yang berupa bahan-bahan hukum, peneliti juga menggunakan bahan-bahan nonhukum apabila dipandang perlu.[14]

Pendekatan penelitian yang digunakan oleh peneliti dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual *(conceptual approach*). Sumber bahan hukum yang digunakan adalah sumber bahan hukum primer, sekunder serta bahan nonhukum. Bahan hukum primer yang digunakan penulis terdiri dari (1) Undang-undang Nomor 10 Tahun 1998 tentang Perbankan; (2) Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi; (3) Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan; (4) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; dan (5) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Bahan hukum sekunder yang digunakan berupa buku, jurnal ilmiah, artikel-artikel, skripsi, maupun makalah terkait maupun *website* yang memiliki relevansi dengan masalah yang diambil yakni perlindungan data oleh penyedia layanan dalam *cloud computing* ditinjau dari UU ITE. Sedangkan bahan nonhukum yang digunakan penulis antara lain bahan nonhukum yang berkaitan dengan *cloud computing*, Kamus Besar Bahasa Indonesia (KBBI) dan kamus hukum *Black's Law Dictionary.*

Sumber-sumber bahan hukum tersebut kemudian dikaji dan dianalisis dengan bantuan teori-teori yang telah didapatkan sebelumnya. Kegiatan analisis bahan hukum ini memberikan telaah, yang dapat berarti menentang, mengkritik, mendukung, menambah atau memberi komentar dan kemudian membuat suatu kesimpulan terhadap hasil penelitian dengan pikiran peneliti sendiri dan bantuan teori yang telah dikuasai.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Beberapa kasus kebocoran data yang dialami perusahaan-perusahaan teknologi besar dunia menjadi peringatan pula bagi perusahaan-perusahaan teknologi lokal bahwa risiko yang sama bisa saja dialami sewaktu-waktu. Risiko-risiko tersebut bisa berasal dari faktor internal maupun eksternal penyedia layanan yang mana hal itu menimbulkan kekhawatiran bagi pengguna. Risiko tersebut di antaranya; (1) *Service Level*, yaitu adanya kemungkinan adanya *service performance* yang tidak konsisten dari penyedia layanan. (2) *Privacy*, yaitu risiko diaksesnya data pengguna oleh pengguna lain karena penggunaan layanan *cloud computing* secara bersama-sama; (3) *Compliance*, yaitu risiko adanya penyimpangan level *compliance* dari penyedia layanan terhadap regulasi yang telah diterapkan oleh pengguna layanan; (4) Data *Ownership*, yaitu risiko kehilangan kepemilikan data begitu data tersimpan di dalam *cloud* yang merupakan milik dari penyedia layanan; (5) Data *Mobility*, yaitu risiko terjadinya kemungkinan *sharing* data antar penyedia layanan *cloud computing* serta mekanisme untuk memperoleh kembali data jika suatu saat pengguna ingin melakukan proses terminasi terhadap layanan *cloud computing* yang tersedia.

[12] Sinta Dewi Rosadi. 2015. *CYBERLAW: Aspek Data Privasi menurut Hukum Internasional, Regional, dan Nasional.* Bandung: Refika Aditama, hal 104.

[13] H. Zainudi Ali. 2009. *Metode Penelitian Hukum,* Jakarta: Siinar Grafika Jakarta, hal. 30.

[14] Peter Mahmud Marzuki. 2014. *Penelitian Hukum. Jakarta: Prenada Media Group,* hal 183.

UU ITE sebagai payung hukum kegiatan elektronik di Indonesia belum mengatur secara jelas bagaimana perlindungan data dilakukan oleh pihak-pihak yang terkait. Hal tersebut menimbulkan kekhawatiran bagi pengguna mengenai siapa yang bertanggung jawab dan bagaimana pertanggungjawaban pihak-pihak terkait. Ketidakpastian hukum ini dapat menghambat perkembangan pemanfaatan teknologi *cloud computing* di negara Indonesia.

Kementerian Komunikasi dan Informatika mengumumkan revisi UU ITE pada Desember 2016 pada beberapa pasal. Perubahan tersebut dituangkan dalam Siaran Pers Kementerian Komunikasi dan Informatika No. 83/HM/KOMINFO/11/2016 Tentang Revisi Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Meskipun beberapa pasal diubah dan ditambahkan beberapa ketentuan, revisi UU ITE di atas masih belum mengakomodasi perlindungan data berupa dokumen elektronik. Kepastian hukum dalam pemanfaatan *cloud computing* dapat terganggu karena tidak adanya norma hukum yang mengatur.

Pembahasan

Kewajiban Melindungi Data Pengguna Layanan *Cloud computing* oleh Penyedia Layanan *Cloud computing* Ditinjau dari UU ITE

Fenomena kebocoran data dalam layanan *cloud computing* menjadi perhatian khusus bagi pengguna maupun penyedia layanan karena data menjadi komoditas utama dalam pemanfaatannya. Penyedia layanan sebagai pemegang peran penting dalam mengelola data di *cloud*, sudah seharusnya menjalankan kewajiban dalam menjaga keamanan dan kerahasiaan data pengguna. Di Indonesia, ada kekhawatiran mengenai perlindungan data karena belum ada undang-undang yang jelas mengatur tentang hal tersebut. Peningkatan dan pengembangan ilmu pengetahuan dan teknologi, globalisasi, dan kekuatan media telah mendesak kebutuhan akan perlindungan data di media elektronik.

Perlindungan data di media elektronik diwujudkan melalui perlindungan hukum yang disusun dalam sebuah peraturan perundang-undangan. Perlindungan hukum ini dimaksudkan untuk memberikan kepastian hukum. Berkaitan dengan perlindungan data dalam layanan *cloud computing*, perlindungan hukum dilaksanakan melalui dua tahap, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif merupakan perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban. Menentukan kewajiban-kewajiban perlindungan data yang harus dilakukan oleh penyedia layanan *cloud computing* merupakan upaya preventif yang dimaksudkan untuk mencegah pelanggaran. Kewajiban hukum tersebut juga menjadi rambu-rambu dan juga batasan-batasan bagi penyedia layanan *cloud computing* dalam menjalankan praktik bisnisnya.

Selain perlindungan preventif, perlindungan represif juga diperlukan dalam hal terjadinya pelanggaran-pelanggaran atas pelindungan data. Meskipun setiap penyedia layanan *cloud computing* berusaha yang terbaik untuk melindungi data pengguna dengan mematuhi kewajiban-kewajiban hukumnya, namun tidak menutup kemungkinan bahwa penyedia layanan masih bisa mengalami peristiwa kebocoran data. Dalam rangka mengantisispasi hal tersebut, perlindungan represif dibutuhkan untuk mengatur bagaimana tanggung jawab penyedia layanan *cloud computing* dalam memberikan kerugian materiil maupun immateriil yang diderita pengguna. Perlindungan hukum represif merupakan perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran.

Sebagai *negara* yang mengemban tugas untuk mewujudkan kesejahteraan rakyatnya, Indonesia mempunyai tugas dan tanggung jawab untuk menjamin berlangsungnya kegiatan pemanfaatan teknologi *cloud computing* agar dapat berjalan secara optimal dan efektif. Penjelasan umum UU ITE menyebutkan bahwa "...untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan teknologi informasi menjadi tidak optimal."

Pengaturan perlindungan data yang berkaitan dengan layanan *cloud computing* tidak dapat ditemukan dalam satu peraturan yang komperehensif. UU ITE yang mengatur dan memfasilitasi penggunaan dan transaksi informasi melalui media elektronik merupakan payung hukum yang dijadikan landasan dalam penyelenggaraan layanan *cloud computing* di Indonesia.

Terkait dengan perlindungan data, untuk memberikan rasa aman bagi pengguna sistem *cloud computing*, dalam UU ITE diatur mengenai perlindungan atas data privasi yang tertuang dalam Pasal 26 ayat (1) yang 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." Sebagaimana tercantum dalam Pasal 26 UU ITE, penggunaan setiap informasi dan data seseorang melalui media elektronik yang dilakukan tanpa persetujuan pemilik data tersebut adalah pelanggaran. Meskipun demikian, ketentuan dalam pasal di atas masih mengatur perlindungan data terbatas pada data pribadi

seseorang. UU ITE belum secara jelas mengatur perlindungan data berupa dokumen elektronik yang tersimpan dalam sistem *cloud computing.*

Menurut Erwin Kuncoro yang merupakan Presiden Direktur Virtus Indonesia, sebuah perusahaan teknologi di Indonesia mengatakan bahwa mengenai regulasi, sistem *cloud* tak lepas dari aturan siapa yang bisa mengaksesnya, dan bagaimana data disimpan. [15] Merujuk pada pernyataannya tersebut, dapat dilihat bahwa dari sisi penyedia layanan pun, regulasi mengenai bagaimana data disimpan dalam sistem *cloud* diperlukan untuk kelangsungan bisnis para penyedia layanan, karena dengan demikian, masyarakat Indonesia bisa segera bermigrasi untuk menggunakan layanan *cloud* tanpa adanya rasa kekhawatiran akan keamanan dan integritas datanya.

Penyedia layanan *cloud computing* sebagai pemegang peran penting dalam perlindungan data pengguna memiliki keharusan untuk menjaga keamanan dan kerahasiaan data dalam menjalankan pelayanannya. Pasal 12 ayat ayat (1) huruf b PP PSTE menyebutkan bahwa "Penyelenggara Sistem Elektronik wajib menjamin (b) tersedianya perjanjian keamanan informasi terhadap jasa layanan Teknologi Informasi yang digunakan." Pasal tersebut menunjukkan bahwa penyedia layanan elektronik sebagai penyedia layanan *cloud computing* secara implisit juga wajib menjaga keamanan data penggunanya. Namun, pasal tersebut tidak menyebutkan secara eksplisit tentang perlindungan data dalam sebuah sistem *cloud computing.* Pasal dalam PP PSTE tersebut menyebutkan bahwa penyelenggara sistem elektronik dalam hal ini termasuk penyedia layanan *cloud computing* diberikan kebebasan membentuk suatu perjanjian keamanan informasi dengan penggunanya. Apabila perlindungan data serta mekanismenya tidak disebutkan dalam suatu peraturan yang jelas, maka hal itu bisa saja digunakan penyedia layanan untuk membuat klausul-klausul yang lebih memihak terhadap mereka. Pengguna sistem layanan *cloud computing* yang berada di tingkat tawar yang lemah pada umumnya langsung menyetujui perjanjian baku yang dibuat oleh penyedia layanan.

Regulasi tentang kewajiban-kewajiban yang harus dilakukan oleh penyedia layanan *cloud computing* dalam rangka perlindungan data pengguna diperlukan dalam rangka memberikan kepastian hukum. Sejumlah ahli hukum mengemukakan prinsip-prinsip perlindungan data yang wajib ditaati oleh pihak-pihak yang berkaitan dengan perlindungan data dalam konsep sistem *cloud computing* adalah penyedia layanan *cloud.* Aan Covoukian menyebutkan pendapatnya yang disebut *privacy by design* yang mana mengandung tujuh prinsip dasar perlindungan data. [16] *Privacy by Design* merupakan suatu teori baru yang menitikberatkan pada pendekatan teknologi dan juga praktik bisnis untuk mengatur perlindungan data. Jadi perlindungan data tidak cukup melalui regulasi tapi juga harus diikuti oleh sistem teknologi informasi, praktik bisnis penyedia layanan yang selalu melindungi dan memerhatikan hak-hak pengguna dan infrasturktur yang mendukung. Beberapa prinsip tersebut sebagai berikut: (1) Proaktif, artinya penyedia layanan sebagai penyelenggara sistem elektronik harus mempersiapkan semua alat, sarana, infrastruktur, praktik bisnis untuk melindungi data sebelum timbul kerugian. Proaktif bukan reaktif, mencegah bukan memperbaiki [17] . Prinsip ini mengedepankan kesiapan penyedia layanan dalam rangka melindungi data pengguna yang dikelolanya sejak awal melalui fasilitas, peralatan teknologi, teknik sarana maupun prasarana. (2) *Default-setting*, menurut prinsip ini, untuk memastikan bahwa data yang diberikan oleh pengguna secara otomatis tersimpan dan terlindungi secara aman dalam sistem. [18] Begitu data diunggah ke sistem penyelenggara elektronik, pengguna tidak perlu melakukan apapun untuk melindungi datanya. Hal itu sudah secara *default* atau diatur otomatis untuk disimpan dan dilindungi dalam sistem teknologi informasi yang disediakan penyelenggara sistem elektronik. Dengan demikian, setiap data yang diunggah pengguna secara *real time* akan tersimpan aman di layanan; (3) *Design-embedded*, artinya perlindungan data disediakan dalam desain teknologi informasi dan ada dalam kebijakan perusahaan dan praktik bisnis. Perlindungan data merupakan bagian integral sistem, tanpa mengurangi fungsi. Jadi dari sisi penyedia layanan, perlu dirancang bagaimana perlindungan data yang mereka tanamkan dalam sistem mereka; (4) *Full functionally*, prinsip ini berusaha mengakomodasi kepentingan pihak-pihak. Bukan hanya dari sisi pengguna saja, namun kepentingan penyelenggara sistem elektronik berusaha diakomodasi berdasarkan prinsip *'win-win solution'.* Perlindungan data merupakan kewajiban penyelenggara sistem elektronik, namun itu semua tidak akan berlangsung optimal tanpa peran dari pengguna layanan *cloud* sebagai pemilik data. Pihak-pihak tersebut wajib melakukan porsi perannya dalam perlindungan data. (5) *End-to-end security*, artinya *Privacy by Design* yang telah tertanam ke dalam sistem

[15] Rachmatunisa. 2014. *Adopsi Lambat, Bisnis Cloud Tetap Melesat,* (http://inet.detik.com/read/2014/06/22/125316/2615424/319/adopsi-lambat-bisnis-cloud- tetap-melesat, diakses 27 Oktober 2016)

[16] Aan Cavoukian. 2014. Privacy by Design. (https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf) dalam Sinta Dewi Rosadi, *Op.cit.,* hal.21

[17] 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem. 2010. Resolution on Privacy by Design, (makalah

[18] *Ibid.*

sebelum elemen pertama dari informasi yang dikumpulkan, menjangkau seluruh siklus hidup data yang terlibat, dari awal sampai akhir. (6) *Visibility and transparancy—keep it open*, artinya bahwa *Privacy by Design* yang berusaha meyakinkan semua pihak bahwa setiap praktik bisnis atau teknologi yang terlibat sesuai dengan janji-janji dan tujuan yang dinyatakan; Bagian komponen dan operasi tetap terlihat dan transparan. Keterbukaan penyedia layanan dalam batas-batas tetentu mengenai bagaimana mereka menjalankan sebuah layanan dapat meningkatkan kepercayaan penggunanya. Kebijakan yang dibuat sewaktu-waktu perlu diinformasikan kepada pengguna khusunya yang akan menimbulkan dampak terhadap kepentingan pengguna; (7) *Respect the user*, artinya menghargai pengguna dengan selalu memberikan informasi tentang kebijkan privasi dan kemudahan pengguna untuk dapat mengerti kebijakan privasi tersebut.

Adapun prinsip-prinsip perlindungan data yang juga dikemukakan oleh Abu Bakar Munir, pengajar di Universitas Malaya Kuala Lumpur yang terdiri dari enam prinsip yang harus ditaati oleh pihak-pihak terkait.[19] Prinsip-prinsip tersebut merupakan prinsip yang memuat tentang konsep perlindungan data yang bertujuan untuk meminimalisir segala bentuk pelanggaran yang mungkin bisa terjadi. Prinsip-prinsip tersebut berkaitan dengan teknologi *cloud computing* dipaparkan sebagai berikut: (1) Prinsip umum, menurut prinsip ini negara harus mengatur mengenai hal umum dalam perlindungan data. Hal-hal umum tersebut meliputi hal-hal fundamental yang wajib dipatuhi oleh pihak-pihak terkait perlindungan data dalam melaksanakan kewajibannya. Negara sebaiknya meletakkan dasar-dasar bagaimana perlindungan data harus dilakukan sehingga pihak–pihak yang berkepentingan memiliki acuan dalam menjalankan praktik bisnisnya. Kemudian turunan dari prinsip umum ini bisa ditentukan sendiri sebagaimana kebutuhan dalam menyelenggarakan layanan *cloud computing;* (2) *Disclosure principle*, artinya pengguna yang menggunakan layanan *cloud computing* boleh meminta informasi mengenai di mana lokasi data disimpan. Karena teknologi *cloud computing* yang bersifat global dan lintas negara, ada beberapa perusahaan yang bekerja sama dengan perusahaan di luar negeri dalam menyediakan *data center*. Sehingga, perusahaan lokal menyediakan pelayanan di mana *data center* berada di luar wilayah Indonesia. Berdasarkan prinsip ini, penyedia layanan *cloud computing* wajib memberitahukan informasi mengenai letak *data center* mereka kepada pengguna; (3) *Security principle*, prinsip ini menghendaki penyedia layanan untuk melindungi data pengguna seperti dari pencurian, *hack*, kebakaran dan resiko lain yang mungkin diderita penyedia layanan; (4) Prinsip retensi, prinsip retensi ini mengatur mengenai jangka waktu suatu data dapat dimusnahkan; (5) Integritas data, prinsip ini meminta penyelenggaa sistem elektronik untuk tetap menjaga data yang dikelolanya tetap utuh dan dimutakhirkan. Berkaitan dengan sistem *cloud computing*, pengguna seringkali mengakses data untuk kemudian diubah. Antara pengguna dengan penyedia layanan, akan selalu terjadi transfer data yang dilakukan melalui internet. Berdasarkan prinsip integritas, *server* penyedia layanan yang menampung dan menyimpan data pengguna seharusnya menjaga keutuhan data mengikuti aktivitas data pengguna; (6) Prinsip akses, penyelenggara sistem elektronik harus memastikan bahwa pengguna dapat mengakses datanya yang disimpan di *server* layanan sewaktu-waktu.

Pemaparan mengenai prinsip-prinsip perlindungan data di atas menunjukkan bahwa penyedia layanan *cloud computing* berperan penting dalam melindungi data penggunanya. Melalui peraturan hukum perlindungan data yang jelas, masalah keamanan data dapat dipecahkan sehingga timbul kepercayaan di antara penyedia layanan maupun pengguna. Kerugian yang mungkin diderita juga dapat dihindarkan.

Beberapa pasal dalam UU ITE maupun PP PSTE sedikitnya telah mengatur beberapa hal mengenai perlidungan data yang semestinya dilakukan pada penyedia layanan *cloud computing.* UU ITE yang saat ini menjadi rujukan mengenai perkembangan teknologi informasi dan komunikasi belum mengakomodasi jaminan keamanan *cloud computing*, demikian halnya dengan PP PSTE. Meskipun terdapat sedikit pasal yang menyebutkan ketentuan tentang perlindungan data, namun dalam perkembangannya, pasal-pasal tersebut masih belum bisa mengakomodasi kekhawatiran pengguna akan datanya di *cloud*. Kewajiban-kewajiban yang semestinya dilakukan oleh penyelenggara sistem elektronik dalam hal ini penyedia layanan *cloud computing* belum terdapat dalam UU ITE maupun PP PSTE. Negara Indonesia melalui regulasinya, perlu untuk membuat sebuah peraturan yang jelas mengenai perlindungan data oleh penyelenggara sistem elektronik agar tumbuh kepercayaan antara pelanggan dan penyedia jasa. Sehingga pemanfaatan teknologi informasi dan komunikasi di Indonesia dapat berjalan secara efektif dan optimal.

Tanggung Jawab Hukum Penyedia Layanan *Cloud Computing* Terhadap Perlindungan Data Pengguna Layanan *Cloud computing* Ditinjau dari UU ITE

Kebocoran data merupakan risiko yang paling dikhawatirkan pengguna layanan elektronik berkaitan

[19] Abu Bakar Munir. 2010. *Personal Data Protection in Malaysia: Law Practice, Op. Cit., Hal 23.*

dengan data yang disimpannya. Data yang telah diunggah ke *server* penyedia layanan *cloud computing* bisa saja hilang dalam dalam awan. Kemungkinan penyedia layanan diretas ataupun tindakan lain juga mengiringi penggunaan teknologi ini. Pengguna yang mempercayakan pengelolaaan atas data yang dimilikinya kehilangan kendali penuh atas datanya yang telah di simpan di *cloud.*

Penyelenggaraan sistem elektronik telah diatur dalam UU ITE dan PP PSTE yang menjadi tonggak lahirnya payung hukum baru dalam pengaturan masalah pemanfaatan informasi dan transaksi elektronik. UU tersebut mengatur aspek-aspek penting dalam pemanfaatan informasi dan transaksi elektronik. Dalam konteks penyelenggaraan sistem elektronik, UU ITE Pasal 15 menyebutkan:

a) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
b) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
c) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal tersebut mengamanatkan bahwa penyelenggara sistem elektronik dalam hal ini temasuk juga penyedia layanan *cloud computing* memiliki tanggung jawab terhadap kelangsungan sistem elektronik yang dijalankannya. Mengelola data pengguna sampai dengan menjaga keamanan serta kerahasiaan data termasuk juga dalam ruang lingkup tanggung jawab penyedia layanan elektronik. Perlindungan data pengguna menjadi agenda penting yang wajib dilaksanakan oleh penyedia layanan *cloud computing* untuk mencegah kemungkinan-kemungkinan yang dapat menimbulkan kebocoran data. Namun, apabila masih terjadi kemungkinan buruk tersebut, Pasal 15 UU ITE huruf b dan c menyebutkan bahwa segala tanggung jawab dibebankan kepada penyedia layanan kecuali penyedia layanan bisa membuktikan bahwa kerugian tersebut bukanlah kesalahannya. Selanjutnya dalam Pasal 13 PP PSTE disebutkan bahwa "Penyelenggara Sistem Elektronik wajib menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan." Hal ini menunjukkan bahwa tanggung jawab apabila ada kerugian yang berkaitan dengan perlindungan data elektronik dalam layanan *cloud computing* belum secara jelas diatur melalui perturan perundang-undangan. Sehingga hal tersebut dapat menimbulkan ketidakpastian hukum untuk pengguna layanan *cloud computing* di Indonesia.

Menyangkut tanggung jawab penyelenggara sistem informasi, dalam Pasal 28 disebutkan penyelenggara sistem elektronik bertanggung jawab terhadap pengamanan dan perlindungan sarana dan prasarana sistem elektronik. Jika terjadi kebocoran data dalam layanan *cloud computing* tentunya akan terjadi suatu 'kerugian' baik materil maupun imateril yang mungkin tidak hanya diderita oleh pihak penyelenggara secara langsung melainkan juga oleh pengguna atas peristiwa kebocoran data tersebut. Sebagai konsekuensinya akan timbul suatu tanggung jawab hukum atas gugatan ganti rugi akibat kerusakan sistem tersebut.

Untuk menentukan tanggung jawab tersebut, maka tanggung jawab dapat ditentukan berdasarkan kontrak/perjanjian para pihak, atau tanggung jawab berdasarkan ketentuan dalam undang-undang yang disebut juga sebagai perbuatan melawan hukum (selanjutnya disebut PMH). Tanggung jawab berdasarkan kontrak akan melihat kepada keberadaan klausul-klausul dalam kontrak, seperti kontrak penjualan atau pemasokan perangkat, kontrak penyediaan jasa, atau kontrak lisensi penggunaan *software*. Berkaitan dengan konsep PMH, Pasal 1365 Kitab Undang-Undang Hukum Perdata berbunyi: "tiap perbuatan melanggar hukum, yang membawa kerugian kepada orang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut". Dalam ketentuan pasal tersebut, terdapat unsur-unsur perbuatan melawan hukum, yaitu adanya perbuatan, adanya unsur kesalahan, adanya kerugian yang diderita, serta adanya hubungan kausalitas antara kesalahan dan kerugian.

Pengertian perbuatan melawan hukum yang lebih luas dapat dilihat dalam yurisprudensi *Arrest* Hoge *Raad kasus Cohen-Lindenbaum* [20] , yaitu suatu perbuatan melawan (*onrechmatige daad*) sebagai suatu perbuatan atau kealpaan yang bertentangan dengan hak orang lain, atau atau bertentangan dengan kesusilaan dan keharusan dalam pergaulan hidup. Sehingga terdapat 4 unsur suatu perbuatan dikategorikan sebagai perbuatan melawan hukum, yaitu: (1*)* perbuatan tersebut bertentangan dengan hak orang lain; (2) bertentangan dengan kewajiban hukum sendiri; (3) bertentangan dengan kesusilaan; (4) bertentangan dengan keharusan yang harus diindahkan dalam pergaulan masyarakat.[21]

Apabila melihat pada UU ITE maupun PP PSTE, pengaturan yang jelas mengenai pertanggungjawaban penyedia layanan *cloud computing* terhadap gangguan perlindungan data belum secara jelas disebutkan. Namun pada pasal 15 huruf c UU ITE mengatur bahwa

[20] *Ibid., hal. 369*
[21] Miru, Ahmadi. 2004. *Hukum Perlindungan Konsumen.* Jakarta: Rajawali Pers, hal. 130

penyelenggara sistem elektronik selalu bertanggung jawab atas kerugian kegagalan sistem sampai ia dapat membuktikan bahwa dirinya tidak bersalah (pembuktian terbalik).

Prinsip yang dituangkan dalam UU ITE tersebut merupakan prinsip praduga untuk selalu bertanggung jawab di mana beban pembuktian terletak pada penyedia layanan *cloud computing.* Hal ini juga selaras dengan ketentuan pertanggungjawaban dalam UUPK Pasal 22 di mana pelaku usaha selalu bertanggung jawab akan kerugian yang diderita konsumennya sampai ia membuktikan bahwa ia tidak bersalah. Kesalahan ada apabila memenuhi empat unsur yang telah disebutkan di atas.

Penempatan beban pembuktian kesalahan pada penyedia layanan *cloud computing* tepat dilakukan dalam konteks teknologi informasi dan komunikasi karena tidak mungkin konsumen dapat membuktikan kesalahan yang terjadi pada sistem tersebut, karena sistem tersebut adalah teknologi tinggi *(hi-tech)* yang tidak mungkin dapat dengan mudah mengakses dan mengetahui bagaimana substansi sistem tersebut sebenarnya.[22] Sehingga lebih efektif apabila penyedia layanan yang dibebani beban pembuktian ini.

PENUTUP

Simpulan

Berdasarkan uraian-uraian yang telah dipaparkan diatas maka dalam penelitian ini dapat disimpulkan bahwa: (1) Indonesia masih belum memiliki sebuah peraturan yang mengatur mengenai kewajiban-kewajiban perlindungan data yang seharusnya dilakukan oleh penyedia layanan *cloud computing* terhadap data penggunanya. Akan tetapi, aspek perlindungan data dapat ditemukan dalam beberapa peraturan perundang-undangan. Khusus untuk perlindungan data pribadi yang secara spesifik berada di lingkup media elektronik terdapat dalam UU ITE serta PP PSTE. Agar dapat mengembangkan layanan *cloud computing* secara efisien dan efektif diperlukan regulasi yang lebih komprehensif terutama mengenai kewajiban-kewajiban perlindungan data yang meliputi kewajiban keamanan, retensi data, integritas data, akses data, keterbukaan informasi layanan, serta aspek fundamental perjanjian tingkat layanan yang semestinya dilakukan oleh penyedia layanan *cloud computing;* (2) Terkait dengan tanggung jawab penyedia layanan *cloud computing* terhadap perlidungan data pengguna, penulis melihat bahwa UU ITE maupun PP PSTE belum secara jelas ditentukan bentuk tanggung jawab yang dibebankan kepada penyedia layanan *cloud computing* apabila terjadi kegagalan perlindungan data. Di dalam konteks penyelenggaraan sistem elektronik, Pasal 15 dan Pasal 16 UU ITE, memberikan standar pertanggungjawaban yang bersifat *presumption of liability* karena tidak mungkin penguna dapat membuktikan kesalahan yang terjadi pada sistem khusunya *cloud computing*, karena sistem tersebut adalah teknologi tinggi *(hi-tech)* yang tidak mungkin dapat dengan mudah mengakses dan mengetahui bagaimana substansi sistem tersebut sebenarnya.

Saran

Masukan bagi pemerintah, perlu dibentuk pranata hukum yang secara khusus membahas dan mengatur mengenai perlindungan data agar perlindungan mengenai data dalam layanan *cloud computing* dapat dilaksanakan dengan lebih menyeluruh. Salah satunya dengan mendorong Kementerian Komunikasi dan Informatika untuk mengesahkan Rancangan Peraturan Menteri Tentang Perlindungan Data Pribadi dalam Sistem Elektronik dengan menambahkan ketentuan-ketentuan mengenai kewajiban serta tanggung jawab hukum penyedia layanan *cloud computing* dalam melindungi data berupa dokumen elektronik.

Bagi penyedia layanan *cloud computing*, perlu diperhatikan bahwa keamanan dan kerahasiaan menjadi isu terpenting dalam implementasi *cloud computing* di Indonesia. Dari segi peraturan perundang-undangan, UU ITE maupun PP PSTE belum cukup untuk mengakomodasi perlindungan data yang komprehensif. UU ITE dan PP PSTE tidak mengatur sejauh mana mekanisme perlindungan yang seharusnya dilakukan dan menjadi tanggung jawab penyedia layanan *cloud computing*. Sebelum dikeluarkannya undang-undang atau pengaturan yang lebih komprehensif mengenai perlindungan data maka para penyedia layanan *cloud computing* yang menjalankan praktik bisnisnya di Indonesia sebaiknya mematuhi prinsip-prinsip perlindungan data untuk membangun hubungan kepercayaan kepada pengguna layanan *cloud computing.*

Daftar Pustaka

Buku

Ali, H. Zainudi. 2009. *Metode Penelitian Hukum,* Jakarta: Sinar Grafika Jakarta.

Brainbridge, David. 2004. *Introduction to Computer Law Fifth Edition.* London: Great Britain by Henry Ling.

Departemen Pendidikan Nasional. 2008. *Kamus Besar Bahasa Indonesia Pusat Bahasa.* Jakarta: Gramedia Pustaka Utama

Fajar, Mukti. 2009. *Dualisme Penelitian Hukum Normatif dan Empiris.* Yogyakarta: Pustaka Pelajar.

[22] Edmon Makarim. 2010. *Op. Cit.*, hal. 172.

Fuady, Munir. 2000. *Perbuatan Melawan Hukum; Pendekatan Kotemporer*. Bandung: Citra Aditya Bekti.

Hadjon, Philipus M. 1987. *Perlindungan Hukum Bagi Rakyat di Indonesia.* Surabaya: Bina Ilmu

Jajuli, Sualaeman. 2015. *Kepastian Hukum Gadai Tanah Dalam Islam.* Yogyakarta: Deepublish.

Korean Information Security Agency. 2009. *Keamanan Jaringan dan Keamanan Informasi dan Privasi.* Incheon: United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development.

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

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

Mansur, Dikdik M. Arief. *Cyber Law: Aspek Hukum Teknologi Informasi.* 2005. Bangung: Refika Aditama.

Marzuki, Peter Mahmud. 2008. *Pengantar Ilmu Hukum.* Jakarta Kencana Prenada Media Group.

_____. 2014. *Penelitian Hukum.* Jakarta: Prenada Media Group.

Mertokusumo, Sudikno. 2011. *Kapita Selekta Ilmu Hukum.* Yogyakarta: Liberty.

Millard, Christopher. 2013. *Cloud computing Law.* New York: Oxford University Press.

P. Graw. 2013. *Proceedings of International Conference on VLSI, Communication, Advance Devices, Signals & Systems and Networking.* New Delhi: Springer.

Rahardjo, Satjipto. 2006. *Ilmu Hukum.* Bandung: Citra Adya Bakti.

Riswandi, Budi Agus. 2005. *Aspek Hukum Internet Banking.* Bandung: Rajagrafindo Persada.

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

_____. 2015. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional.* Bandung: Refika Aditama.

Smith, Graham J. H. 2007. *Internet Law and Regulation. London: Sweet & Maxwell*.

Wahana Komputer. 2010. *The Best Encryption Tools.* Jakarta: Elex Media Komputindo.

Wahyudi, Bambang. 2008. *Konsep Sistem Informasi*: *Dari Bit Sampai Ke Database.* Yogyakarta: Andi Offset

Makalah dan Jurnal

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

Berzanson, Randall P. 1992. "The Right to Privacy Revisited: Privacy, News and Social Change. *California Law Review* Vol. 80.

Carroll, Mariana dan Merwe, Alta van der 2011. *Secure Cloud computing Benefits, Risks and Controls* dipublikasikan dalam IEEE (Institute of Electrical and Electronics Engineers).

Hon, W. Kuan, dkk. 2012. Negotiating Cloud Contracts: Looking at Clouds From Both Sides Now. *Stanford Technology Law Review Volume 16, Number 1 Fall.*

Kesan, Jay P., dkk. 2013. "Information Privacy and Data Control in *Cloud computing*: Consumers, Privacy Preferences, and Market Efficiency". *Washington and Lee Law Review.* Vol. 77 (6).

Mell, Peter and Grance, Timothy. 2011. *The NIST Definition of Cloud computing Special Publication 800-145.* Gaithersburg: U.S Department of commerce.

Ryan, Michael dan Leoffler, Christopher M. 2010. "Insights into *Cloud computing*". *Intellectual Property and Technology Law Journal*. Vol. 22 (11).

Sefton, Patrick. 2010. *Privacy and Data Control In the Era of Cloud computing.* Australia: BrightLine Lawyers.

Sugiharto. 2015. *Pendekatan Informasi Sebagai Komoditi Dalam Proses Diseminasi Informasi*, (Online), (www.pdii.lipi.go.id, diunduh 19 April 2016).

Website

Akrim, Red. 2012. *Cloud computing: the 4th IT Industrial Revolution!* (https://www.cloudswave.com/blog/cloud-computing-the-4th-it-industrial-revolution/), diakses 6 Maret 2016.

_____. 2015. *Home Marketing The Growth of Cloud The Growth of Cloud computing in Emerging Asian Market,* (https://www.cloudswave.com/blog/ the-growth-of-cloud-computing-in-emerging-asian-market/), diakses 4 Februari 2016.

Alphabet Inc. 2015. *Alphabet Inc. and Google Inc. Annual Report Form 10-K United States Securities and Exchange Comission*, (https://abc.xyz/investor/pdf/20151231_alphabet_10K.pdf), diunduh 6 Maret 2016.

Australian Government. 2014. *Australian Government Cloud computing Policy*, (http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf), diunduh 5 Maret 2016.

Hutapea, Febriamy. 2014. *Foto Pribadi Bintang Hollywood Kembali Diretas*, (http://www.beritasatu.com/amerika/211481-foto-pribadi-bintang-hollywood-di-icloud-kembali-diretas.html, diakses 8 Maret 2016).

Ratnaning, Asih. 2012. *DropBox Dibobol, Akun Pengguna Dicuri*, (https://tekno.tempo.co/read/news/2012/08/01/072420780/dropbox-dibobol-akun-pengguna-dicuri, diakses 5 Februari 2016.

Santoso, Berkah. 2012. *Cloud-Computing-dan-Strategi-TI-Modern* (http://www.cloudindonesia.or.id/wp-content/uploads/2012/07/ E-Book-Cloud-Computing-dan-Strategi-TI-Modern1.pdf), diunduh 6 Maret 2016.

Tarigan, Insaf Albert. 2014. *Ganti Password, 7 Juta Akun Dropbox Diretas*, (http://teknologi.metrotvnews.com/read/2014/10/15/305077/ganti-password-7-juta-akun-dropbox-diretas), diakses 4 Februari 2016.

Peraturan Perundang-undangan

Kitab Undang-undang Hukum Perdata (KUH Perdata).

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

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Lembaran Negara Republik Indonesia Nomor 154 Tahun 1999, Tambahan Lembaran Negara Republik Indonesia Nomor 3881.

Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Lembaran Negara Republik Indonesia Nomor 154 Tahun 1999, Tambahan Lembaran Negara Republik Indonesia Nomor 3881.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Nomor 58 Tahun 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348.