CyberSecurity dan Forensik Digital e-ISSN: 2615-8442

Vol. 1, No. 2, November 2018, hlm. 39-44

ANALISA KEAMANAN DAN HUKUM UNTUK PELINDUNGAN DATA PRIVASI

Muhammad Na'im Al Jum'ah

Magister Informatika Universitas Islam Indonesia Yogyakarta
Email: [1]naim83fikom@gmail.com,

Abstrak

Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung dengan signifikan. Meskipun penetrasi internet di masyarakat masih sangat kurang bila dibandingkan dengan jumlah total penduduk Indonesia, kini sistem informasi dan komunikasi elektronik telah diimplementasikan pada hampir semua sektor kehidupan dalam masyarakat. Penyalagunaan data juga menjadi perhatian khusus. Banyak pelanggaran data yang terjadi karena implementasi yang buruk atau tidak adanya kontrol keamanan baik di perusahaan swasta maupun di organisasi pemerintahan. Paper ini akan membahas tentang bagaimana pengawasan data privasi dan peraturan hukum mengenai perlindungan data pribadi. Dari hasil analisa tehadap pengawasan data pribadi bahwa ada dua pihak yang mampu dan punya peluang melakukan pengawasan massal, yaitu pihak swasta dan pemerintah. Pihak swasta bisa berasal dari penyedia layanan dan konten online, penyedia layanan internet atau pemilik infrastruktur internet sedangkan tugas negara adalah melindungi serta menjamin hak warganya. Namun pihak pemerintah sering menggunakan keamanan sebagai dalih untuk mendasari tindakan-tindakan yang melanggar hak atas privasi. Indonesia telah memiliki beberapa undang-undang yang mengatur tentang keamanan data privasi duantaranya adalah Undang-undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan, Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-undang Nomor 7 Tahun 1992 jo Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata kunci: *keamanan data, data privasi, hokum data privasi.*

SECURITY AND LEGAL ANALYSIS FOR PRIVACY DATA PROTECTION

Abstract

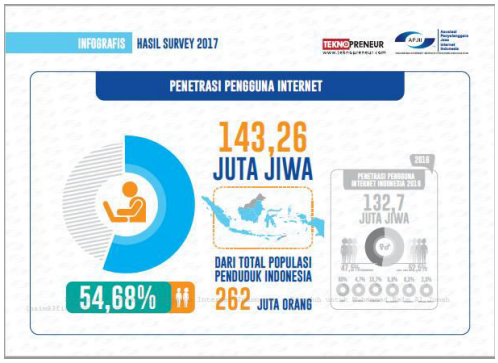
Information technology has changed the lifestyle of people globally and caused significant changes in socio-cultural, economic and legal frameworks. Although internet penetration in the community is still very low compared to the total population of Indonesia, now the electronic information and communication system has been implemented in almost all sectors of life in society. Data misuse is also of special concern. Many data violations occur due to poor implementation or lack of security controls both in private companies and in government organizations. This paper will discuss how to monitor privacy data and legal regulations regarding the protection of personal data. From the results of the analysis on personal data supervision that there are two parties who are able and have the opportunity to conduct mass surveillance, namely the private sector and the government. The private sector can come from online service and content providers, internet service providers or internet infrastructure owners while the state's duty is to protect and guarantee the rights of its citizens. But the government often uses security as a pretext for underlying actions that violate the right to privacy. Indonesia already has several laws governing the security of privacy data, among others, Law Number 7 of 1971 concerning Principal Archival Provisions, Law Number 8 of 1997 concerning Corporate Documents, Law Number 7 of 1992 jo Law Number 10 of 1998 concerning Banking, Law Number 36 of 1999 concerning Telecommunications, Law Number 11 of 2008 concerning Information and Electronic Transactions.

Keywords: *data security, privacy data, privacy data law*

1. PENDAHULUAN

Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung dengan signifikan. Meskipun penetrasi internet di masyarakat masih sangat kurang bila dibandingkan dengan jumlah total penduduk Indonesia, kini sistem informasi dan komunikasi elektronik telah diimplementasikan pada hampir semua sektor kehidupan dalam masyarakat.

Menurut hasil survay dari pada april 2017, jumlah pengguna internet di dunia mencapai 3,811 miliar (Hootsuite, 2017) sedangkan presentase pengguna internet di Indonesia mencapai 54,68% dengan kalkulasi 143,26 juta jiwa merupakan pengguna internet dari total jumlah penduduk Indonesia 262 juta jiwa (Asosiasi Pengguna Jasa Internet Indonesia, (2017).



Gambar 1. Penetrasi pengguna internet Indonesia

Seiring dengan keterbukaan terhadap data dan informasi, maka perlindungan terhadap informasi menjadi hal yang wajib. Dalam beberapa tahun terakhir, perkembangan pesat dan biaya yang lebih rendah dalam teknologi informasi dan komunikasi telah membuatnya lebih mudah diakses dan nyaman. Akibatnya, jumlah pengguna internet telah meledak.

Penyalagunaan data juga menjadi perhatian khusus. Banyak pelanggaran data yang terjadi karena implementasi yang buruk atau tidak adanya kontrol keamanan baik di perusahaan swasta maupun di organisasi pemerintahan. Banyak negara yang berusaha meningkatkan persyaratan kemana dan menerapkanya di undang-undang mereka. Namun, sebagian beasar kerangka keamanan bersifat reaktif dan tidak mengatasi ancaman yang relevan (Sungmi Park, 2018)

Potongan-potongan data dan informasi pribadi ini dapat dimanfaatkan oleh pelaku cbercrime untuk melakukan pengambilan data secara ilegal, tetapi juga dapat digunakan oleh perusahaan yang telah mengumpulkannya dalam batas-batas hukum dan melihatnya sebagai aset perusahaan (Schwartz, 2004). Banyaknya masalah yang muncul akibat dari penyala gunaan data pribadi, maka perlu ada upaya dari pemerintah untuk menerapkan aturan tentang kemanan data pribadi sehingga masalah-masalah ini dapat diantisipasi. Paper ini akan membahas tentang bagaimana pengawasan data privasi dan peraturan hukum mengenai perlindungan data pribadi.

2. PENGAWASAN DATA PRIVASI

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.

Istilah perlindungan data pertama digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur perlindungan data pribadi melalui undangundang. 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 dari pada itu agar penggunaan data pribadi tidak disalahgunakan maka diperlukan pengaturan.

Tiap-tiap negara menggunakan istilah 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. 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.

Menurut Jerry Kang, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karateristik masing-masing individu. Pada dasarnya

bentuk perlindungan terhadap data dibagi dalam dua kategori, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data yang kasat mata maupun data yang tidak kasat mata. 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

Pengawasan Digital (Digital Surveillance) Pengawasan (Surveillance) adalah memantau aktivitas, perilaku, atau proses bertukar informasi yang dilakukan oleh masyarakat dan biasanya dilakukan untuk kepentingan seperti mempengaruhi, mengatur, mengarahkan, atau melindungi mereka. Dalam konteks digital, pengawasan seperti yang dilakukan dengan penyadapan, dilakukan dengan memanfaatkan teknologi digital dan jaringannya. Mengingat infrastruktur internet dan perusahaan-perusahaan penyedia layanan serta konten cenderung terpusat dan berada dalam pengaruh Amerika Serikat, tentu informasi yang dibocorkan oleh Snowden menjadi lebih masuk akal.

Ada dua pihak yang mampu dan punya peluang melakukan pengawasan massal, yaitu pihak swasta dan negara (pemerintah). Pihak swasta bisa berasal dari penyedia layanan dan konten online, penyedia layanan internet atau pemilik infrastruktur internet. Motivasinya bisa karena ingin mengetahui perilaku online pelanggannya atau informasi lain yang bisa menguntungkan perusahaan tersebut. Sedangkan pihak negara biasanya diwakili oleh lembaga penegak hukum atau badan intelijen. Pengintaian ini biasanya dilakukan untuk memantau potensi tindakan kriminal, terorisme, atau bahkan untuk mengawai oposisi pemerintah (aktivis, jurnalis, dll). Seperti yang telah dibocorkan oleh Snowden, pengawasan tidak hanya berlaku di satu teritori, tetapi juga lintas teritori. Pengawasan massal secara global dilakukan oleh 'Five Eyes' (Lima Mata) yaitu meliputi: NSA milik pemerintah Amerika Serikat, Communications Security Establishment (CSE) milik pemerintah Kanada, Global Communications Headquarter milik pemerintah Britania Raya, Defense Signals Directorate (DSD) lembaga pemerintah Australia, dan pemerintah Selandia Baru dengan Government Communications Security Bureau (GCSB).

Internet memiliki infrastruktur yang berbeda dengan medium komunikasi yang pernah ada sebelumnya, contohnya: surat, telepon. Saluran komunikasi sebelumnya memiliki infrastruktur yang terpisah satu sama lainnya. Dengan keberadaan internet, kebutuhan mengirim pesan, menelepon, dan bahkan membaca berita, semua dilakukan dalam satu infrastruktur jaringan. Semua aktivitas komunikasi tersebut dikirim menjadi suatu paket data yang ditransfer melalui jaringan. Hal ini memudahkan pengintai untuk memata-matai aktivitas komunikasi seseorang hanya dengan satu saluran. Faktanya, meskipun seseorang ingin mengirim surel dari Jakarta ke Belanda, jika pengirim dan penerima menggunakan layanan milik perusahaan Amerika Serikat, lalu linta pengiriman akan melewati infrastruktur di negara tersebut sebelum sampai ke penerima. Infrastruktur tulang punggung (backbone) internet juga cenderung terpusat.

Banyak jalan untuk mengintip apa yang sedang kita lakukan di internet. Bisa dengan menyadap melalui tulang punggung internet, kerjasama dengan pemilik kabel serat optik, dan cara lain yang mampu mengintip isi paket data dalam proses perpindahan. Cara tersebut dikenal sebagai Upstream Collection. Berdasarkan dokumen yang dibocorkan oleh Snowden, operasi pengawasan memasang perangkat keras yang berfungsi untuk mengawasi di berbagai titik pemeriksaan dalam tulang punggung internet. Selain cara tersebut, dengan teknologi seperti Deep Packet Inspection (DPI), yang mampu memeriksa lalu lintas internet secara otomatis berdasarkan kata kunci atau kode tertentu. Meskipun teknologi ini bisa digunakan untuk mencegah virus atau serangan yang bisa merusak lalu lintas, ada berbagai bukti juga bahwa DPI digunakan oleh pemerintah untuk kepentingan tertentu. Pada tahun 2013, pemerintah Malaysia yang dikuasai oleh Barisan Nasional contohnya, menggunakan DPI untuk menyadap lawan politiknya dalam masa menjelang pemilu.

Tugas negara adalah melindungi serta menjamin hak warganya. Pihak pemerintah sering menggunakan keamanan sebagai dalih untuk mendasari tindakan-tindakan yang melanggar hak atas privasi. Faktor-faktor seperti terorisme, kejahatan di dunia maya, atau ancaman bagi negara mendorong program pengawasan massal. Sedangkan pihak swasta, memanfaatkan pengawasan untuk keuntungan perusahaannya, misalnya untuk mengalahkan kompetitornya lewat jalur belakang atau membatasi pilihan pengguna internet. Di sesi sebelumnya kita juga sudah membahas pentingnya kontrol pribadi terhadap segala informasi dan data yang kita punya. Dengan adanya pengawasan massal, kontrol tersebut berpindah tangan ke

perusahaan dan negara. Keduanya ingin membangun profil pribadi dari serpihan data yang mereka kumpulkan, profil tersebut akan menjadi sasaran dalam mencapai kepentingan mereka. Negara memang wajib menjamin keamanan warganya, tapi kalau negara justru membatasi dan bisa membahayakan warganya, tentu lain cerita. Seperti pemerintah Republik Rakyat Cina yang selalu mengawasi seluruh warganya, membatasi ekspresi warga dan berusaha menyingkirkan lawan politiknya.

Keberadaan program seperti ini menjadikan kekuasaan semakin terpusat dan melakukan tindakan semena-mena. Konsekuensinya, memudahkan pemerintah untuk menjadi otoriter dan melanggar hak asasi manusia warganya. Privasi dan kebebasan berekspresi saling berkaitan, jika ada seorang jurnalis yang mengungkap kasus korupsi diawasi terus-menerus oleh lawannya, besar kemungkinan dirinya dan bahkan keluarganya berada dalam bahaya. Dengan kenyataan bahwa internet bukan dunia impian yang merdeka dan bebas campur tangan dari pemerintah dan pihak lainnya, masihkah kamu berpendapat bahwa tidak ada yang perlu ditakuti jika tidak ada yang kamu sembunyikan?

Patut dicatat, bahwa privasi bukan semata soal rahasia atau menyembunyikan informasi tertentu. Privasi adalah tentang otonomi, kuasa, dan kontrol yang memungkinkan kita untuk memutuskan bagaimana kita ingin memperlihatkan diri kita (myshadow.org) . Pelanggaran privasi bahkan bisa berdampak pada risiko lanjutan seperti kehilangan kesempatan pekerjaan, hanya karena satu kesalahan yang pernah kamu lakukan di masa lampau muncul di internet, memberi peluang untuk cyber-bullying, dituduh atas sesuatu yang belum tentu kamu lakukan, serta risiko lainnya.

3. PERATURAN PEMERINTAH TENTANG PERLINDUNGAN DATA PRIVASI

Indonesia merupakan salah satu negara berkembang memiliki jumlah pengguna teknologi dan sistem komunikasi modern yang sangat besar. Kehadirat internet telah mengubah cara pandang manusia untuk berkomunikasi, karena dapat meruntuhkan batas-batas negara. Teknologi informasi telah merubah pola hidup masyarakat secara global menyebabkan perubahan sosial, budaya, ekonomi, dan kerangka hukum yang berlangsung secara signifikan.

Namun hingga kini Indonesia belum memiliki hukum yang secara spesifik mengatur mengenai perlindungan privasi dan data. Akibatnya dengan meningkatnya pemanfaatan teknologi, urgensi untuk mengatasi permasalahan hukum yang terkait dengan perlindungan privasi dan data menjadi meningkat. Hal ini disebabkan karena seringkali hukum yang sudah ada tidak dapat bekerja secara efektif dalam mengikuti perkembangan teknologi. Hukum seringkali berjalan lebih lambat dibandingkan dengan perkembangan masyarakatnya, termasuk juga perkembangan teknologi.

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 kesehatan18. 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.

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).

Di Indonesia pengaturan secara khusus mengenai perlindungan data memang belum ada, namun aspek perlindungannya sudah tercermin dalam peraturan perundang-undangan lainnya62 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, Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.1. UU No.8 Tahun 1997 tentang Dokumen Perusahaan.

Undang-undang No.8 Tahun 1997 ini adalah undang-undang yang mengatur tentang data perusahaan. Pada pasal 1 ayat 2 menjelaskan bahwa dokumen perusahaan adalah data, catatan, dan atau keterangan yang dibuat dan atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya,

baik tertulis di atas kertas atau sarana lai maupun terekam dalam bentuk corak apapun yang dapat dilihat, dibaca, atau didengar.

3.2. UU No. 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan

Dalam undang-undang No. 7 tahun 1971 tentang ketentuan pokok kearsipan pada Bab IV tentang Kewajiban Kearsipan pasal 9 dijelaskan bahwa: (1)Arsip Nasional Pusat wajib menyimpan, memelihara dan menyelamatkan arsip sebagaimana dimaksud dalam pasal 2 huruf b Undang-undang ini dari Lembaga-lembaga Negara dan Badan-badan Pemerintahan Pusat. (2)Arsip Nasional Daerah wajib menyimpan, memelihara dan menyelamatkan arsip sebagaimana dimaksud dalam pasal 2 huruf b Undang-undang ini dari Lembaga-lembaga Negara dan Badan-badan Pemerintahan Daerah serta Badan-badan Pemerintah Pusat di tingkat Daerah. (3)Arsip Nasional Pusat maupun Arsip Nasional Daerah wajib menyimpan, memelihara dan menyelamatkan arsip yang berasal dari Badan-badan Swasta dan/atau perorangan.

3.3. UU No. 10 Tahun 1998 tentang Perbankan

Dalam undang-undang ini di jelakan pada pasal 1 poin 28 menjelaskan bahwa Rahasia Bank adalah segala sesuatu yang dengan keterangan mengenai nasabah penyimpan dan simpanannya. 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 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

3.4. UU No. 36 Tahun 1999 tentang 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.

3.5. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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 UndangUndang ini. Penjelasan Pasal 26 Ayat (1) menerangkan bahwa dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights)

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. Berdasarkan UU ITE ini juga, setiap orang dilarang dengan cara apapun untuk membuka informasi milik orang lain dengan tujuan apapun bahkan jika data yang sifatnya rahasia sampai dapat terbuka kepada publik. Lebih jauh, perlindungan terhadap data tidak hanya mengatur akses pembukaan data saja, tetapi juga apabila data dapat dibuka dan diubah dengan cara apapun (manipulasi, perubahan, pernghilangan, pengrusakan) sehingga seolah-olah data tersebut menjadi data otentik.

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A. 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

4. KESIMPULAN

Ada dua pihak yang mampu dan punya peluang melakukan pengawasan massal, yaitu pihak swasta dan negara (pemerintah). Pihak swasta bisa berasal dari penyedia layanan dan konten online, penyedia layanan internet atau pemilik infrastruktur internet. Tugas negara adalah melindungi serta menjamin hak warganya. Pihak pemerintah sering menggunakan keamanan sebagai dalih untuk mendasari tindakan-tindakan yang melanggar hak atas privasi.

Indonesia telah memiliki beberapa undang-undang yang mengatur tentang keamanan data privasi duantaranya adalah Undang-undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan, Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-undang Nomor 7 Tahun 1992 jo Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

DAFTAR PUSTAKA

SUNGMI PARK dkk, 2018. A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement.

Asosiasi Pengguna Jasa Internet Indonesia, 2018.

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

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

https://kemudi.xyz/static/web/modul/[lores]%20modul%204%20EBookModulKEMUDI.pdf

https://www.merdeka.com/teknologi/apa-itu-cambridge-analytica-dan-haruskah-kita-tinggalkan-facebook-selamanya.html

HUI ZHU dkk, 2017. Information dissemination model for social media with constant updates.

JOINSON, A, dkk. 2010. "Privacy,Trust and Self Disclosure Online." Human Computer Interaction (25) 1-24.

KUMAR N, dkk. 2016. On Privacy and Security in Social Media – A Comprehensive Study.

KANG, JERRY. 1998. “Information Privacy in Cyberspace Transaction” Stanford Law Review Vol 50.

MAKARIM, EDMON. 2005. Pengantar Hukum Telematika (Suatu Kompilasi Kajian). Jakarta: RajaGrafindo Persada.

MAULANA, ADHI, Tingkat Kejahatan Cyber Di Indonesia Sudah Gawat, http://tekno. liputan6.com/read/2019078/tingkat-kejahatan/cyber-di-indonesia-sudah-gawat, 6 agustus 2018

NUGRAHA, (2012). Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undangundang Informasi Dan Transaksi Elektronik.

PURWANTO, 2007. “Penelitian Tentang Perlindungan Hukum Data Digital”. Jakarta : Badan Pembinaan Hukum Nasional.

SITOMPUL, ASRIL. 2001. Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace, Bandung: PT.Citra Aditya Bakti.

Undang-undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan.

Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.

Undang-undang Nomor 7 Tahun 1992 jo Undang-undang Nomor 10 Tahun 1998 tentang Perbankan.

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.