Perlindungan Data Personal Siber di Indonesia

Wisnu Handi Prabowo

Program Studi Hubungan Internasional FISIP Universitas Padjadjaran, Indonesia;

email: wisnu15001@mail.unpad.ac.id

Satriya Wibawa

Departemen Hubungan Internasional FISIP Universitas Padjadjaran, Indonesia;

email: satriya.wibawa@mail.unpad.ac.id

Fuad Azmi

Departemen Hubungan Internasional FISIP Universitas Padjadjaran, Indonesia;

email: fuad.azmi@mail.unpad.ac.id

Dikirim:

30 Juni 2019

Direvisi:

14 Oktober 2019

Diterima:

28 Januari 2020

Dipublikasikan:

31 Januari 2020

Keywords

*Cyber Security, Data Sovereignty,
Human Security, Indonesia
Private Data*

ABSTRACT

This research is motivated by the occurrence of cases of data breach that occurred in Indonesia, where Indonesia with a large number of Internet users has encouraged the growth of foreign technology companies participation in Indonesia. This technology company collects and processes data taken from internet users in Indonesia which being saved on their data servers abroad. This use of personal data has affected the security of individual privacy of Indonesian user.

This study aims to explain the protection of data that has been carried out by the Government of Indonesia and its impact on the vital core of the Indonesian human security population. The concept of human security and cyber security is used to explain the potential threats posed by the policies that have been carried out by the state and their impact on the vital core of the Indonesian population. This study uses a qualitative method.

Kata Kunci

*Data Sovereignty , Data Pribadi,
Human Security, Indonesia,
Keamanan Siber*

ABSTRAK

Penelitian ini dilatarbelakangi oleh terjadinya kasus kebocoran data yang terjadi di Indonesia, dimana Indonesia dengan jumlah pengguna Internetnya yang besar telah mendorong pertumbuhan perusahaan teknologi asing untuk berpartisipasi di Indonesia. Perusahaan teknologi ini mengumpulkan dan mengolah data yang diambil dari pengguna internet di Indonesia di server data di luar negeri. Sehingga pemanfaatan data pribadi yang memengaruhi keamanan privasi individu.

Penelitian ini bertujuan untuk menjelaskan perlindungan terhadap data yang telah dilakukan oleh Pemerintah Indonesia dan dampaknya terhadap vital core dari human security penduduk Indonesia. Pendekatan yang digunakan adalah konsep human security dan keamanan siber untuk menjelaskan potensi ancaman yang ditimbulkan dari kebijakan yang telah dilakukan negara dan dampaknya terhadap vital core penduduk Indonesia. Penelitian ini menggunakan metode kualitatif.

PENDAHULUAN

Kehidupan manusia telah mengalami perubahan dalam signifikan pada masa globalisasi. Globalisasi didefinisikan sebagai sebuah proses sosial yang menghilangkan batasan geografi dalam ekonomi, politik, sosial dan kultur. Dimana masyarakat menjadi semakin peka terhadap apa yang terjadi dan bertindak dengan menyesuaikan diri (Waters, 1995, hal. 5). Kepekaan tersebut sangat dipengaruhi oleh kemudahan arus informasi yang mudah diakses oleh manusia di berbagai belahan dunia. Informasi yang didapat tersebut, tidak terbatas pada media masa konvensional seperti surat kabar, radio dan televisi. Namun, keberadaan informasi digital seperti yang tersedia melalui internet. Telah memberikan kesempatan yang lebih bagi para individu untuk mengakses informasi secara cepat. Sehingga, hambatan dalam bentuk batas wilayah menjadi hal yang bisa diatasi secara mudah.

Dalam Globalisasi yang terjadi, aktivitas sosial, politik dan ekonomi dalam suatu tempat dapat memengaruhi kondisi individu dan komunitas di negara lain. Sehingga dalam proses yang disebut deteritorialisasi ini, batas-batas yang ada dalam ruang lingkup wilayah fisik semakin memudar (McGrew, 2014, hal. 19).

Hal tersebut dapat terlihat melalui aktivitas kolaborasi yang menghubungkan berbagai tempat di dunia dalam berbagai bidang kegiatan. Munculnya proses yang disebut dengan *flattening*¹ ini, telah menunjukkan bahwa pembatas fisik semakin bisa diatasi melalui teknologi yang dapat diakses oleh masyarakat umum. Akses yang mudah ini, juga memberikan kesempatan bagi individu ataupun kelompok serta memberikan kesempatan terhadap negara berkembang

untuk meningkatkan pembangunan perekonomiannya, melalui pemanfaatan teknologi yang memberikan kesempatan yang dapat mengejar ketertinggalan dari negara maju (Friedman, 2005).

Selanjutnya, berkaitan dengan aktivitas yang semakin intensif dalam kegiatan yang menghubungkan kegiatan non-fisik dengan dunia fisik dalam teknologi informasi, istilah Cyberspace atau ruang siber perlu dipertimbangkan. Ruang siber dapat diartikan sebagai lingkungan dimana data digital dibentuk, disimpan, dan dibagi. Tidak terbatas hubungannya dalam dimensi virtual, tetapi juga fisik dalam bentuk sistematis alat penyimpanan data dan infrastruktur yang memengaruhinya (Singer & Friedman, 2014, hal. 14).

Apabila dihubungkan dengan tingkat kejahatan siber yang terjadi di dunia. Pada tahun 2013, dalam laporan Akamai International tahun 2013, Indonesia menempati peringkat kedua sebagai negara launchpad serangan siber (Akamai Technologies, 2014). Penempatan Indonesia sebagai negara tertinggi kedua dalam hal sumber serangan siber menunjukkan pengelolaan terhadap ruang siber yang lemah. Kelemahan yang signifikan ini berpotensi menimbulkan kerugian terhadap berbagai aktivitas yang berhubungan dengan dunia virtual.

Selain kerugian diterima korporasi, masyarakat Indonesia secara luas juga terancam oleh serangan siber Ancaman kerugian tersebut dapat bersumber dari luar maupun dalam negeri.

Dampak dari ketidak-amanan dalam ruang siber Indonesia ini dapat mengancam berbagai kelompok dan individu di Indonesia. Berdasarkan penelitian yang dilakukan oleh Microsoft yang membahas mengenai serangan siber yang terjadi pada tahun 2017 di Indonesia. Akibat dari ketidaksiapan keamanan siber, terdapat ancaman terhadap keberlangsungan operasional perusahaan maupun karyawannya.

¹ Proses dimana persaingan kompetisi akan melibatkan partisipasi dari negara industri dan negara berkembang, enterprener individu dan perusahaan baik pemain besar dan kecil akan bersaing dalam kesempatan yang sama.

Sejak tahun 2003, Kementerian Komunikasi dan Informasi di bawah kepemimpinan Syamsul Mu'arif sudah mulai merancang peraturan yang dapat melindungi hak-hak pengguna internet di Indonesia dari kejahatan digital. Perancangan peraturan ini juga melibatkan kementerian lain di pemerintahan, serta bekerja sama dengan Universitas Negeri Padjadjaran, Institut Teknologi Bandung dan Universitas Indonesia. Hal tersebut terwujud pada dengan keluarnya UU ITE (Undang-Undang no 11 Tahun 2008) yang disahkan pada 25 Maret 2008. Namun, setelah disahkannya peraturan ini, terdapat berbagai permasalahan yang muncul. Undang-undang yang seharusnya melindungi hak-hak masyarakat Indonesia, justru menjerat berbagai kegiatan mengutarakan pendapat warga Indonesia (Rudiantara, 2016).

Selanjutnya mengenai penelitian terhadap perlindungan siber, terdapat beberapa penelitian yang membahas perlindungan di Indonesia dan membahas berbagai kelemahan yang ada, terutama dalam perlindungan hukumnya. Pertama, dalam Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional oleh Akbar Kunia Putra (2014), membahas mengenai isi dari UU ITE ini tidak memberikan pengklasifikasian yang tidak eksplisit mengenai kejahatan siber. Pengaturan dalam UU ITE ini, tidak mengatur kejahatan dalam arti sempit tetapi menyamakannya dengan tindak pidana konvensional.

Kedua, D.D Machmuddin dan B. Pratama (2017) dalam *Some of Indonesia Cyber Law Problems* menjelaskan bahwa pembentukan UU ITE terkesan dibuat terlalu awal dan tidak memperhatikan penempatan media pengaksesan, yaitu komputer maupun variasinya. Pembahasan ini penting karena dapat memberikan konfirmasi jelas mengenai pencurian data yang tergolong kejahatan siber.

Ketiga, Suyanto Sidik (2013) dalam *Dampak Undang-undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat*. Menganalisis mengenai isi dari Undang-Undang yang dapat diadaptasikan

dalam perubahan dalam bidang teknologi. Namun memiliki kekurangan karena cenderung menjadi duplikasi dari hukum konvensional, serta sama sekali tidak membahas mengenai perlindungan terhadap jaminan keamanan dan kerahasiaan di ruang siber.

Keempat, Rini Retno Winarni (2016) dalam *Efektivitas Penerapan Undang-Undang ITE dalam tindak pidana Cyber Crime* membahas mengenai beberapa contoh kelemahan UU ITE. Salah satunya adalah tidak adanya pembahasan mengenai data. Hal ini perlu diperhatikan mengingat potensi bahaya dari leakage and espionage (membocorkan data kendala yuridis dan kendala penanganan spionase) serta yang dapat mengancam masyarakat luas yaitu pencurian identitas virtual.

Kelima, Master Thesis oleh Silja-Madli Ossip (2017) yang berjudul *Cyber threats and cybercrime – a disruption of human security? Membahas mengenai dampak dari kejahatan siber terhadap keamanan individu*. Dampak tersebut dikategorikan berdasarkan jenis target, yaitu personal atau umum (random). Dalam penelitian tersebut dijelaskan mengenai ancaman kejahatan siber yang sulit terdeteksi sebelum kebocoran data terjadi.

Keenam, dalam Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional oleh Akbar Kunia Putra (2014), membahas mengenai isi dari UU ITE ini tidak memberikan pengklasifikasian yang tidak eksplisit mengenai kejahatan siber. Pengaturan dalam UU ITE ini, tidak mengatur kejahatan dalam arti sempit tetapi menyamakannya dengan tindak pidana konvensional.

Ketujuh, D.D Machmuddin dan B. Pratama (2017) dalam *Some of Indonesia Cyber Law Problems* menjelaskan bahwa pembentukan UU ITE terkesan terburu-buru dan tidak memperhatikan penempatan media pengaksesan, yaitu komputer maupun variasinya. Pembahasan ini penting karena dapat memberikan konfirmasi jelas mengenai pencurian data yang tergolong kejahatan siber.

Kedelapan, Suyanto Sidik (2013) dalam Dampak Undang-undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat. Menganalisis mengenai isi dari Undang-Undang yang dapat diadaptasikan dalam perubahan dalam bidang teknologi. Namun memiliki kekurangan karena cenderung menjadi duplikasi dari hukum konvensional, serta sama sekali tidak membahas mengenai perlindungan terhadap jaminan keamanan dan kerahasiaan di ruang siber.

Dari kedelapan penelitian sebelumnya, dapat diketahui bahwa : Empat Penelitian pertama, membahas mengenai kelemahan UU ITE dalam analisis dengan pendekatan ilmu hukum di mana terdapat kekurangan dalam penanganan permasalahan privasi dan informasi. Sementara Penelitian kelima membahas mengenai hubungan di antara human security dengan kejahatan siber. Oleh karena itu, dalam penelitian ini diambil pendekatan berbeda. Digunakan perspektif human security dan keamanan siber untuk menjelaskan potensi ancaman terhadap masyarakat Indonesia.

Berbagai penelitian tersebut digunakan untuk sebagai referensi dan pijakan dalam menjawab rumusan permasalahan “Bagaimana Pemerintah Indonesia melindungi Data Pribadi di Indonesia?”.

KERANGKA KONSEPTUAL

Secara sederhana, human security merupakan jenis keamanan yang memindahkan referent object dari negara menjadi individu. Pemenuhan keamanan akan tercapai apabila kesejahteraan dan martabat manusia telah terpenuhi secara memadai (Tadjbakhsh & Chenoy, 2007, hal. 19). Kesadaran akan perlunya keamanan yang tidak semata berfokus kepada negara, mulai muncul sejak akhir Perang Dunia II. Kasus Holocaust dan Pengadilan Nuremberg telah mendorong diperlukannya pertimbangan terhadap perlindungan terhadap masyarakat dan

penempatannya terhadap kedaulatan negara. Terutama setelah munculnya Piagam Persatuan Bangsa-Bangsa, Deklarasi Universal mengenai Hak Asasi Manusia dan Konvensi Geneva, dimana semuanya mengakui hak dari masyarakat, termasuk hak pribadi (Axworthy, 2001, hal. 19). Namun, dengan terjadinya Perang Dingin yang mengonstruksi dunia dalam keadaan bipolar yang menempatkan negara dalam kondisi yang tegang. Membuat pembahasan mengenai konsep keamanan yang menempatkan masyarakat sebagai referent object, kembali dibahas di akhir Perang Dingin. Hal tersebut merupakan upaya untuk merevisi pengertian keamanan sebagai bentuk dari “derivative of power” yang sangat dikaitkan dengan kondisi Perang dingin yang memperlihatkan negara dalam kondisi selalu memperebutkan “power” (Buzan, 1983, hal. 8-9).

Barry Buzan yang menyadari bahwa konsep keamanan secara pondasi terlalu sempit, menawarkan pendekatan terhadap keamanan dalam tiga level yaitu individu, negara dan sistem internasional. Keberadaan level analisis individu ini, difokuskan kepada hubungan di antara personal security yang dapat memengaruhi entitas level kedua dalam analisis Buzan, yaitu negara. Dalam level ini Buzan, mempertimbangkan ancaman sosial yang dapat muncul karena keterkaitan manusia dengan lingkungannya yang tidak dapat menghindari konsekuensi sosial, ekonomi dan politik yang tidak dapat dihindari. Bentuk dari ancaman ini dapat disederhanakan menjadi empat yaitu ancaman fisik, ancaman ekonomi, denial of acces , threats to rights , ancaman terhadap posisi atau status (Buzan, 1983, hal. 20).

Buzan juga mempertimbangkan kondisi dimana negara dapat menjadi sumber ancaman terhadap penduduknya. Ancaman tersebut diklasifikasikan menjadi empat kategori yaitu: ancaman dari pembentukan dan penegakan hukum domestik, tindakan politik dari negara terhadap individu atau kelompok, perebutan kekuasaan dan kebijakan keamanan eksternal

negara (Buzan, 1983). Keempat kategorisasi tersebut mengklasifikasikan berbagai ketidakstabilan yang terjadi ketika komponen-komponen negara, terutama institusi-institusi formalnya dihadapkan kepada keputusan untuk memprioritaskan kepentingan kolektif atau kepentingan individu. Dalam ancaman bentuk pertama, keamanan individu dapat terancam melalui pelaksanaan hukum yang tidak sempurna. Selanjutnya, dalam ancaman jenis kedua, legitimasi pemerintah untuk menjalankan hukum dapat disalahgunakan untuk mendiskriminasi kelompok tertentu. Selanjutnya dalam ancaman bentuk ketiga, tidak berjalannya mekanisme pergantian kekuasaan yang damai dapat menjadikan negara rawan terhadap ancaman intervensi negara asing. Selain itu, ancaman terorisme dapat memaksa negara untuk merespons melalui tindakan yang mengorbankan keamanan individu. Terakhir, konsekuensi dari kebijakan luar negeri yang dilaksanakan negara, dapat memberikan beban dan ancaman terhadap warga negara. Ancaman paling nyata dalam kategori ini adalah terjadinya perang (Buzan, 1983, hal. 25-27). Meskipun membahas mengenai ancaman terhadap individu. Buzan menolak konsep keamanan yang terlalu luas dan menolak dimasukkannya hak asasi manusia dalam keamanan (Buzan, 2004, hal. 369-370).

Namun, perkembangan politik pada awal 1990-an telah memungkinkan terjadi optimisme akan terjadinya kedamaian yang stabil. Sehingga terdapat pengembangan keamanan yang meninggalkan garis-garis keamanan tradisional. Amartya Sen dalam Human Development Report 1993, mendefinisikan human development sebagai proses dari meluasnya kesempatan manusia untuk memutuskan pilihan dalam kehidupannya. Maka, Human Security dapat diartikan sebagai masyarakat yang dapat mengimplementasikan pilihannya secara aman dan bebas. Sehingga mereka memiliki kepercayaan bahwa pilihan yang dimiliki sekarang tidak akan musnah pada masa mendatang. Dalam laporan ini, terdapat empat

karakteristik utama, yaitu: universal concern, interdependent, yang terjamin dalam upaya perlindungan dan bersifat people-centered. Laporan ini memberikan saran untuk dilakukannya perluasan yang radikal terhadap pendefinisian keamanan yang lebih mementingkan kepentingan masyarakat yang terkategorisasikan dalam ketujuh kategori yaitu ekonomi, pangan, kesehatan, lingkungan, personal, komunitas dan politik. Keamanan ekonomi membutuhkan adanya kepastian lapangan pekerjaan yang mendukung pendapatan dasar. Keamanan pangan berhubungan dengan kesempatan bagi semua orang untuk mengakses kebutuhan pangan dasar. Keamanan kesehatan berhubungan dengan pengadaan pangan dalam menghadapi tantangan nutrisi yang rendah, penyakit mematikan dan sejenisnya (Shinoda, 2004, hal. 9). Penelitian ini, kemudian menjadi fondasi kuat dalam kemunculan Human Security sebagai konsep, pada United Nations Development Programme's (UNDP) 1994 Human Development Report. Dalam laporan ini, terdapat konseptualisasi keamanan yang luas serta meninggalkan pendekatan state-centrism.

Lahirnya konseptualisasi ini, disebabkan oleh Referent object yang ditetapkan terhadap negara, terbukti tidak sesuai untuk menganalisis adanya konflik perang sipil yang terus bermunculan pasca Perang Dingin. Kemudian dengan mengutamakan negara, maka hal tersebut dapat menghindarkan fakta bahwa upaya mencapai keamanan negara sering mengorbankan keamanan individu. Oleh karena itu, Human Security merupakan pengembalian kembali fokus keamanan kepada masyarakat, dimana hal tersebut telah muncul sebelum generasi hak politik, hak sosial dan ekonomi dan rights of difference (Tadjbakhsh & Chenoy, 2007, hal. 74).

Human Security akan membawa isu ekonomi dan pembangunan secara bersamaan dengan isu militer dan keamanan. Konsep ini telah menjadi isu yang diakui secara internasional sejak tahun 1994, yaitu sejak publikasi UNDP. Dikeluarkannya laporan ini

juga diikuti dengan adaptasi yang dilakukan oleh berbagai cabang organisasi Persatuan Bangsa-Bangsa (PBB) yang menempatkan Human Security sebagai agenda utama. Di bidang akademis sendiri, Human Security telah diadopsikan di berbagai pemikiran realis, liberal, teori kritikal dan konstruktivis yang berusaha memberikan pendefinisian yang jelas agar bisa diintegrasikan ke dalam perencanaan penelitian (Elias & Sutch, 2007, hal. 162 - 163).

Melalui penetapan individu sebagai referensi maka dalam perspektif ini akan dianggap bahwa keselamatan dari individu merupakan kunci untuk mencapai keamanan global. Implikasinya, ketika keamanan individu terancam maka keamanan internasional juga terancam (Hampson, Daudelin, Hay, Reid, & Martin, 2002, hal. 6).

Terutama dengan kondisi sistem internasional yang mengarah kembali mengarah ke dalam kondisi Hobbesian, membuat kembali diperhatikannya garis-garis keamanan tradisional dan hubungan di antara keamanan dan pembangunan mendapat perhatian (M.Shaw, J.MacLean, & R.Black, 2006, hal. 3). Keterkaitan di antara keamanan negara dan keamanan populasinya akan saling memengaruhi.

Taylor Owen menjelaskan bahwa dalam melihat human security tidak bisa dipahami sebagai pilihan di antara ancaman luas atau sempit, melainkan sebagai *threshold of severity* (batasan terhadap kekerasan). Melalui pendekatan yang diusulkannya, segala ancaman yang ada di lokasi mana pun akan dianggap sebagai ancaman terhadap human security, apabila mengancam terhadap *vital core* yang dimiliki oleh individu, terutama dari ancaman yang kritis dan meluas (Martin & Owen, 2014, hal. 5). Pembatasan Owen ini akan selaras dengan pandangan Sabina Alkire yang berpendapat bahwa tujuan dari human security adalah untuk menjaga "*vital core*" dari segala bentuk ancaman yang meluas, yang pelaksanaannya konsisten dengan pemenuhan jangka panjang manusia. Adapun yang

dimaksud dengan "*vital core*" adalah hak dan kebebasan yang berkaitan dengan kelangsungan hidup, mata pencaharian dan martabat (reputasi dalam tingkat mendasar). Pengertian ini didasarkan oleh alasan praktis yang digunakan untuk mengklasifikasikan prosedur dalam berbagai bentuk terhadap pengertian *freedom from fear* dan *freedom from want* yang bersifat luas (Alkire, 2003, hal. 2).

Kemudian untuk mengetahui mengenai Batasan-batasan dalam Human Security, perlu memahami konsep-konsep seperti *vital core* dan orientasi yang berfokus kepada masyarakat. *Vital core* merujuk kepada istilah non-teknis yang dapat diartikan *sebagai space of capability, the freedom people have to do and to be*. Elemen dari *vital core* ini, dianggap sebagai hak-hak yang fundamental sehingga semua pihak dan institusi memiliki kewajiban untuk menjaganya, meskipun kemampuan yang dimiliki tidak memungkinkan untuk melaksanakan hal tersebut secara sempurna. Adapun mengenai pertimbangan di antara memprioritaskan hak dengan kapabilitas, akan sangat diperlukan institusi yang memberikan keputusan yang adil. Oleh karena itu akan sangat diperlukan partisipasi dari institusi maupun pihak yang haknya terancam.

Konsep dari human security yang sangat luas, dapat memberikan keuntungan dalam menganalisis permasalahan yang muncul di era pasca perang dingin ini. Pendekatan holistik dalam human security, dapat memfasilitasi dibahasnya berbagai isu yang sebelumnya tidak mendapat perhatian. King dan Murray (2001 : 589) telah mendeskripsikan konsep dari human security sebagai "*unifying event*" dan berfungsi sebagai konsep yang memungkinkan dilakukannya kerja sama pada isu keamanan yang disetujui. Pada masa sebelumnya, kerja sama dalam penanggulangan isu keamanan terhambat oleh sifat keamanan tradisional yang sempit (terutama dalam membahas isu keamanan *high politic*) yang menghalangi terjadinya kooperasi. Secara lebih lanjut, Tadjbakhsh dan

Chenoy (2007: 10), beranggapan bahwa pendefinisian yang luas dan fleksibel dari human security merupakan pilihan yang layak. Hal tersebut dikaitkan dengan pendekatan holistik yang akan memberikan pemahaman yang baik terhadap berbagai isu di era modern yang saling berkaitan.

Selain itu, Wiben (2011), menganggap bahwa analisis melalui human security telah memperkaya pemikiran keamanan melalui deepening (memperhitungkan kepentingan pribadi dan tidak terbatas kepada negara), widening (memperhitungkan jenis ancaman lain dan tidak terbatas kepada ancaman kekerasan), memberdayakan dari bawah (diamankan oleh siapa?, menggunakan instrumen jenis apa?) dan memiliki perhatian signifikan terhadap dimensi subjektif terhadap persepsi dan agensi (siapa yang memersepsikan keamanan?) (Gasper & Gómez, 2015, hal. 6).

Human security yang memberikan kesempatan bagi partisipasi aktor non-negara, telah memungkinkan dilakukannya jenis diplomasi terbaru. Dalam jaringan ini berbagai aktor dengan pemikiran yang sama telah mendorong PBB untuk meningkatkan perlindungan terhadap warga negara. Jaringan ini didukung bermula dari perjanjian bilateral di antara Kanada dan Norwegia yang berkoalisi dengan dengan berbagai negara di seluruh dunia dan didukung oleh organisasi internasional, untuk membentuk The Human Security Network (Axworthy, 2001, hal. 20). Partisipasi Non-Governmental Organization (NGO) dan organisasi kemasyarakatan yang memiliki keahlian teknis dan pengalaman yang sangat penting di era modern ini. Dapat diakomodasi oleh konsep human security (Axworthy, 2001, hal. 23).

Secara spesifik, apabila dihubungkan dengan keamanan pribadi. Des Gasper dan Oscar A. Gómez dalam menganalisis laporan UNDP 1994, Personal security meliputi berbagai keamanan yang diklasifikasikan ke dalam:

- *Security from violence* yang berasal dari ancaman terhadap

kehidupan dan kepemilikan, dari kecelakaan, penyiksaan (termasuk self-abuse, menggunakan obat-obatan terlarang) dan ditelantarkan,

- *Economic Security* yang meliputi pekerjaan dengan pendapatannya serta ketersediaan tempat tinggal,
- *Community Security* yang berkaitan dengan konflik dalam suatu komunitas, berkaitan dengan penduduk asli suatu daerah dan sejenisnya,
- *Political Security* yang ditujukan terhadap dasar dari hak asasi manusia terutama yang berkaitan dengan hak sipil dan politik.

Berbagai jenis ancaman tersebut, dalam Human Development Report 1994 telah terbagi ancaman ke dalam tiga jenis, yaitu: ancaman dari eksternal atau internal; ancaman internal terhadap pemerintahan, selain konflik bersenjata, dalam bentuk variasi kejahatan baik dilakukan oleh negara atau lainnya; Ancaman terhadap diri sendiri, berkaitan dengan bunuh diri dan penggunaan obat-obat terlarang (Gasper & Gómez, 2015, hal. 8). Pentingnya personal security dalam human security, dianggap sebagai fase pertama dalam ekspansi dari konsep human security, bukan sebagai pembatas hal ini berkaitan dengan perubahan pola konflik bersenjata dan menurunnya konflik bersenjata secara umum (Gasper & Gómez, 2015, hal. 9).

KEAMANAN SIBER

Cybersecurity atau keamanan siber, dapat diartikan sebagai segala hal yang berkaitan dengan teknologi dan proses yang bertujuan untuk melindungi sistem komputer, perangkat lunak dan pengguna dari akses yang tidak memiliki izin, yang bentuk ancamannya berasal dari para pelaku kejahatan siber, kelompok teroris dan hacker. Perlindungan ini diterapkan pada peralatan-peralatan dan jaringan yang menjadi tempat aktivitas

ekonomi dan mendapatkan informasi (Comodo, 2018).

Kemudian apabila didefinisikan secara luas yang berkaitan dengan berbagai kegiatan-kegiatan umum di kehidupan sehari-hari. Keamanan siber dapat dikaitkan dengan tiga hal berikut: satu jenis kegiatan atau tindakan yang ditujukan untuk melindungi jaringan komputer dengan perangkat keras dan lunak yang menyimpan informasi dan media komunikasi dari serangan, gangguan atau bentuk ancaman lainnya ; Kondisi yang menggambarkan perlindungan dari ancaman (siber) ; Mencakup bidang luas yang memiliki tujuan untuk mengimplementasikan dan meningkatkan kualitas dari berbagai kegiatan (perlindungan) tersebut (Fischer, 2016, hal. 1).

Tujuan dari keamanan siber apabila dikaitkan dengan eksistensi informasi dalam ruang siber akan sangat memprioritaskan tiga hal yaitu Confidentiality, Integrity dan Availability. Confidentiality berhubungan dengan menjaga privasi data. Hal tersebut dikaitkan dengan keadaan dunia digital yang menilai informasi sebagai hal yang berharga, terlebih apabila dikaitkan dengan identitas pemilik sumber informasi tersebut dan relasinya dengan pihak lain. Integrity berkaitan dengan berbagai alat teknis seperti enkripsi, kontrol akses dan perlindungan legal. Terakhir Availability berhubungan dengan kepercayaan bahwa sistem dan data tidak diubah tanpa sepengetahuan atau persetujuan. Terdapat ekspektasi sistem berjalan seperti biasa (Singer & Friedman, 2014, hal. 35). Ketiga hal ini akan diimplementasikan ke dalam berbagai upaya pengamanan dalam hal teknis maupun non-teknis.

Kemudian dalam kaitannya dengan Cyberspace (ruang siber). Perlu dipahami bahwa ruang siber tidak terbatas pada internet saja. Dalam memahami ruang siber ini , perlu dibedakan dengan Internet yang berkaitan dengan terhubungnya perangkat keras dalam komunikasi standar protokol ataupun World Wide Web (WWW) yang menggambarkan

terhubungnya hypertext document melalui internet. Sedangkan Ruang Siber sendiri harus dipahami sebagai metafora yang menggambarkan keterhubungan berbagai alat yang menggunakan teknologi komputer yang saling bertemu (Betz & Stevens, 2011, hal. 13). Pertemuan ini terjadi dalam satu dimensi virtual. Dalam dimensi ini berbagai alat yang terhubung dalam internet akan memengaruhi kehidupan nyata atau fisik, dan apa yang terjadi dalam dimensi fisik dalam partisipasi kegiatan akan memengaruhi dalam dunia virtual. Sehingga, ruang siber tidak bisa dipisahkan dengan dimensi fisik. Apa yang terjadi di dunia fisik akan memengaruhi dunia virtual secara signifikan dan sebaliknya.

Selanjutnya dari perspektif sosial, ruang siber terkonstruksi dalam hal terjadinya interaksi. Interaksi yang tercipta ini merupakan hal yang tercapai dari inisiatif keterhubungan alat dalam internet. Sebagai bagian dari ruang siber, internet telah menjadi komponen yang membentuk ruang siber melalui tersambungannya jutaan komputer dalam jaringan global. Dalam jaringan ini, keterhubungan diantara komponen-komponen fisik telah membentuk kerangka logika yang memungkinkan terjadinya proses manipulasi, eksploitasi dan augmentasi terhadap informasi ketika terjadinya interaksi. Dalam interaksi ini, terdapat karakteristik desentralisasi di antara aktor dengan kepentingannya yang saling memengaruhi (Choucri, 2013, hal. 4). Dalam sifatnya yang terdesentralisasi inilah terdapat peluang yang luas bagi berbagai golongan, baik individu dan kelompok untuk melaksanakan kepentingan yang mereka miliki.

Untuk membedakan dengan dimensi lainnya, maka perlu untuk memperhatikan dari tiga atribut dan dampak dari ruang Siber. Pertama, adanya ketidaktahuan mengenai identitas dan lokasi dari aktor karena terdapat peluang untuk menggunakan alias dan proxy yang sulit untuk diketahui karena didukung oleh arsitektur fisik dan software. Kedua, terdapat peningkatan kecepatan, volume dan

jangkauan komunikasi. Selain negara dan korporasi, individu secara global dapat menggunakannya. Selain itu sifat demokratis dari pengembangan teknologi telah mendukung penyebarluasan penggunaan teknologi. Terakhir, hambatan dalam memasuki ruang siber semakin berkurang, dengan penurunan biaya serta kemudahan mendapatkan teknologi yang memberikan akses terhadap internet. Hal ini akan berpotensi mengganggu status quo. Semua pihak dapat berpartisipasi dengan kepentingannya masing-masing. Kelompok militer dengan teknologinya yang canggih dapat memanfaatkan ruang siber sebagai medan pelaksanaan strategi. Namun, pada waktu bersamaan juga terdapat peluang untuk meningkatkan kesejahteraan dalam peredaran barang dan jasa. Serta memberikan peluang kepada warga negara untuk berpartisipasi dalam komunitas social (Betz & Stevens, 2011, hal. 9-10).

METODE RISET

Dalam penelitian ini, penulis menggunakan metode penelitian kualitatif. Menurut John W Creswell pada bukunya yang berjudul *Research Design : Qualitative, Quantitative, and Mixed Methods Approaches* (2014), penelitian kualitatif adalah sebuah pendekatan untuk mengeksplorasi dan memahami arti dari individu atau kelompok yang melekat pada masalah sosial humaniora. Proses dari penelitian meliputi pertanyaan, data dengan settingan peserta, analisis data secara induktif serta pembuatan interpretasi arti data yang dilakukan oleh peneliti. Laporan akhir tertulisnya memiliki struktur yang sangat fleksibel.

Metode kualitatif bergantung kepada data dalam bentuk teks dan gambar. Metode ini memiliki langkah-langkah yang khas dalam menganalisis data dan berada dalam rancangan yang bervariasi (Creswell, 2014). Dalam penelitian ini, permasalahan yang akan diteliti adalah bagaimana perlindungan siber terhadap privasi masyarakat Indonesia. Perlindungan ini akan berkaitan dengan pengaruh yang

ditimbulkan dari kebijakan negara terhadap keamanan masyarakat Indonesia. Terutama dalam hal efektifitas perlindungan terhadap keselamatan warga Indonesia ketika berpartisipasi dalam ruang siber.

Peneliti menggunakan metode penelitian kualitatif karena metode ini dinilai mampu membantu peneliti dalam memahami dan mengeksplorasi masalah penelitian secara mendalam dengan beberapa upaya utama, yaitu: 1.) pengajuan beberapa pertanyaan dan prosedur, 2.) pengumpulan data yang spesifik, 3.) analisis data, serta 4.) penafsiran makna data (W.Creswell, 2009, hal. 4-5). Melalui langkah-langkah yang diambil tersebut, penelitian berusaha menjelaskan secara deskriptif kekurangan yang dimiliki oleh UU ITE 2008 dalam melindungi keamanan siber warga Indonesia. Pendeskripsian mengenai kekurangan tersebut kemudian akan dikembangkan melalui pendekatan studi kasus (W.Creswell, 2009, hal. 19-21). Pendekatan studi kasus merupakan pendekatan kualitatif yang berusaha mengembangkan dan mengeksplorasi pemahaman secara lebih mendalam mengenai suatu kasus untuk diilustrasikan secara spesifik melalui pengumpulan data-data yang lengkap yang bersumber dari informasi beragam, meliputi, wawancara, materi audio dan visual serta berbagai bentuk dokumen maupun laporan (W.Creswell, 2009, hal. 73). Pemilihan pendekatan studi kasus ini akan memberikan keuntungan bagi peneliti untuk mendalami permasalahan yang ada dalam suatu kasus karena sifatnya yang mengembangkan deskripsi dan analisis. Sehingga eksplorasi perlindungan human security dalam perspektif siber akan memberikan kemudahan kepada peneliti.

Dalam bukunya, Cresswel menyebutkan langkah-langkah pengumpulan informasi dilakukan melalui observasi dan interview yang bersifat semi terstruktur maupun tidak berstruktur, dokumen dan hal-hal berbentuk visual atau informasi berbentuk rekaman. Dalam upaya untuk memperoleh data ini, akan

difokuskan kepada wawancara kualitatif dan studi pustaka.

Pelaksanaan wawancara kualitatif bertujuan untuk mendapatkan data primer, dimana akan terjadi tatap muka dengan responden yang dipilih. Namun, apabila wawancara tatap muka tidak dimungkinkan. Wawancara tidak langsung melalui telepon ataupun media komunikasi lain akan menjadi pilihan kedua. Dalam proses wawancara ini peneliti telah menyiapkan daftar calon narasumber yang memiliki kepakaran sesuai dengan penelitian. Narasumber tersebut adalah:

- Satriyo Wibowo, Konsultan di Kementerian Komunikasi dan Informatika, Cyberlaw Community.
- Onno W. Purbo, Dosen Fakultas Ilmu Institut Informatika dan Bisnis Darmajaya.
- Budi Rahardjo, Ketua Indonesia Computer Emergency Response Team (ID-CERT)
- Ashwin Sasongko Sastrosubroto Dirjen Aplikasi Informatika Kementerian Komunikasi dan Informasi
- Didik Hardiyanto, Sandiman Muda Subdirektorat Proteksi Keamanan Informasi Publik, Direktorat Proteksi Ekonomi Digital, Deputy Proteksi Badan Siber dan Sandi Negara.

Pada penelitian ini, peneliti akan mengumpulkan data melalui dua sumber yaitu sumber primer dan sumber sekunder. Dalam mengumpulkan data primer, peneliti akan menggunakan wawancara narasumber yang memahami atau terlibat langsung dengan topik penelitian. Wawancara narasumber primer tersebut kemudian akan menghasilkan data primer bagi penelitian ini. Sementara pengumpulan data sekunder dilakukan dengan melakukan studi pustaka.

Selanjutnya, mengenai sumber data kedua yaitu sumber data sekunder akan dilakukan

melalui studi pustaka. Studi pustaka ini akan dilakukan melalui pengumpulan dan analisis terhadap berbagai jurnal, buku, halaman web resmi, e-book maupun laporan resmi yang diberikan oleh institusi terpercaya.

HASIL DAN PEMBAHASAN

Kewajiban dan komitmen Pemerintah dalam Perlindungan Data

Dalam upaya perlindungan terhadap data pribadi, dikenal istilah data protection. Data protection secara umum didefinisikan sebagai hukum yang dibuat untuk melindungi data pribadi seseorang. Di dalam masyarakat modern, untuk mengangkat kemampuan manusia dalam mengontrol data dan melindungi manusia dari penyalahgunaan. Maka, sangat penting bagi dibentuknya hukum perlindungan data untuk mengatur kegiatan perusahaan dan pemerintah yang berperan aktif. Kedua institusi ini, merupakan institusi yang berperan dalam pencegahan penyalahgunaan data. Namun, tidak adanya peraturan dapat memberikan kemudahan terhadap kegiatan eksploitasi data yang dapat dilakukan oleh pihak lain (Privacy International, 2019, hal. 9).

Di Indonesia tidak terdapat peraturan peraturan perundangan yang memberikan penjelasan secara eksplisit mengenai 'privasi'. Namun, dalam pasal 28 ayat 1 Undang-Undang 1945 terdapat berbagai hak yang berkaitan erat dengan hak privasi. (ELSAM & International, 2016, hal. 3)

Namun apabila dilihat dari partisipasi negara di berbagai forum internasional. Indonesia telah menjadi negara yang menyetujui berbagai peraturan internasional yang secara eksplisit maupun implisit memberikan perlindungan terhadap data pribadi maupun privasi.

Persetujuan terhadap praktik perlindungan data Pribadi, disetujui dalam bentuk prinsip internasional oleh berbagai negara, praktik, keputusan, rekomendasi dan pembentukan

kebijakan. Berbagai instrumen kebijakan ini telah muncul secara signifikan dalam:

- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), tahun 1981 yang diamandemenkan pada tahun 2018.
- The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) yang diamandemen pada tahun 2013.
- The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).
- Peraturan lain seperti APEC Privacy Framework - Asia-Pacific Economic Cooperation.

Keberadaan berbagai instrumen ini dapat mengharuskan berbagai perusahaan yang melakukan pengumpulan data harus bersedia untuk tunduk kepada hukum yang telah ditetapkan di negara tersebut. Berbagai praktik perlindungan data akan mengandung upaya perlindungan terhadap individu melalui pembatasan keleluasaan para pengkoleksi data dengan cara yang adil, legal dan transparan, dijelaskannya tujuan dari penggunaan data (Privacy International, 2019, hal. 14-16). Meskipun menjadi salah satu negara yang menghadiri kesepakatan dalam forum-forum tersebut, Indonesia belum terikat terhadap peraturan internasional yang dapat mendorong bagi kemajuan signifikan terhadap perlindungan data pribadi penduduknya.

Terlepas dari belum adanya peraturan khusus yang dapat melindungi warga negaranya dalam hal privasi di ruang siber Indonesia telah memiliki kewajiban dan komitmen untuk melindungi hak asasi. Artikel 12 dari Universal Declaration of Human

Rights (UDHR). UDHR sendiri dibentuk sebagai dasar dalam pembuatan perjanjian hak asasi internasional. Peraturan ini memiliki persamaan dengan International Covenant on Civil and Political Rights (ICCPR) yang menginspirasi hak untuk berprivasi. (ELSAM & Privacy International, 2016, hal. 2). Maka secara tidak langsung perlindungan terhadap hak asasi akan berkaitan dengan perlindungan terhadap privasi.

Selanjutnya, mengenai keterkaitan diantara privasi dengan kebebasan berpendapat dan berekspresi. Pada tahun 2011, the then-UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression mengeluarkan laporan yang menjelaskan “ perlindungan data pribadi merupakan representasi dari penghargaan terhadap hak untuk berprivasi.....Tidak ada satupun individu dikenakan pemberlakuan hukum yang akan mengganggu privasi dirinya, keluarga, rumah ataupun dalam berkomunikasi.....setiap orang memiliki hak untuk mendapat perlindungan dari hukum terhadap berbagai gangguan ataupun serangan. Perlunya untuk mengadopsi hukum yang jelas untuk melindungi data pribadi perlu ditingkatkan pada era informasi saat ini, dimana terdapat volume data yang dikoleksi dan disimpan lewat perantara. Selain itu terdapat kekhawatiran bahwa berbagai negara menetapkan kewajiban atau bahkan memaksa terhadap berbagai perusahaan swasta untuk memberikan informasi dari pengguna (Privacy International, 2019, hal. 10).

Berbagai program dan penelitian yang dilakukan oleh PBB tersebut mendapat perhatian dalam UN General Assembly tahun 2016, yang telah mensahkan resolusi yang didasarkan kepada consensus mengenai Hak untuk mendapatkan privasi dalam dunia digital (GA Resolution 71/1991) yang mengokohkan keputusan resolusi sebelumnya yang membahas pada subjek tersebut, menguatkan bahwa: Negara harus menghargai hak asasi manusia internasional dan harus mematuhi kewajiban yang berkaitan dengan hak untuk berprivasi, yaitu ketika terdapat permintaan

untuk mengungkapkan atau memberitahukan data pribadi yang dimiliki oleh pihak ketiga (perusahaan swasta). Hal ini menunjukkan bahwa privasi dan perlindungan data merupakan hal yang saling berkaitan. Individu, sebagai warga negara, konsumen, pengguna perlu memiliki cara dan alat untuk melaksanakan hak yang dimiliki terhadap privasi yang dimiliki dan melindungi data yang mereka miliki dari penyalahgunaan. Terdapat hal penting yang harus diketahui, bahwa kewajiban dalam pengelolaan data harus jelas. Terdapatnya kejelasan hukum akan membuat para perusahaan ini memiliki langkah mitigasi terhadap gangguan terhadap hak berprivasi. Sehingga apabila terdapat permasalahan terhadap data pribadi yang dikelola, para perusahaan ini dapat dianggap sebagai pihak yang bertanggung jawab.

Penempatan data pribadi sebagai hak fundamental juga terus mendapat perhatian yang meningkat, bahkan dianggap sebagai hal yang terpisah tetapi sama penting dengan hak asasi manusia. Hal ini telah diakui di Eropa dalam Charter of Fundamental Rights of the European Union artikel 8 yang memberikan perlindungan perlindungan data kepada semua pihak, menjamin penggunaan data yang adil dengan akses yang memadai bagi pemilik dan adanya keterlibatan Lembaga independen sebagai pengawas (Privacy International, 2019, hal. 14).

Rezim perlindungan data personal yang ada di dunia, pada umumnya didasarkan kepada konsep informational self-determination, yaitu Individu menentukan data mana yang dapat di share dan untuk siapa dan kepentingan apa. Berdasarkan pemikiran ini, pengguna akan memiliki kekuatan untuk menentukan tingkat privasi yang diinginkan ketika mereka berinteraksi atau menggunakan layanan Google, Facebook dan penyedia layanan teknologi lain. Pemikiran ini, menunjukkan kepercayaan terhadap paradigma perlindungan privasi yang bersifat non politik yang didukung anggapan bahwa perlindungan data pribadi dapat diserahkan kepada peraturan yang

dibuat untuk mengatur kegiatan ekonomi. Sehingga, perusahaan diharapkan untuk menghormati privasi konsumen sebagai upaya untuk tetap kompetitif dalam bisnis.

Namun self-determinasi ini harus diikuti oleh kemampuan untuk mengetahui kapasitas penyimpanan, proses transfer dan pemrosesan terhadap data untuk menentukan persetujuan yang diminta dan penentuan keputusan tersebut harus bebas dari pengaruh eksternal. Hal ini menjadi permasalahan dalam layanan jaringan social, seperti facebook karena kekuatan jaringannya membuat terdapatnya berbagai perusahaan teknologi yang memiliki nyaris memiliki monopoli. Akibatnya apabila berusaha mengisolasi diri dari jaringan. Hal ini membuat upaya mendapatkan privasi semakin sulit ketika infrastruktur social dan teknis terus digitalisasi. Agar individu dapat memiliki control terhadap akan menemui hambatan bagi para kelompok yang memerlukan perhatian khusus seperti anak-anak, orang tua atau orang berkebutuhan khusus. Hal ini akan semakin menguatkan pendapat para ahli yang menyatakan bahwa dengan meningkatnya arus data (Schünemann & Baumann, 2017, hal. 6)

Berbagai rezim yang diikuti ini merupakan langkah negara untuk melindungi data pribadi dan telah diadopsi oleh mayoritas negara di dunia. Meskipun pada umumnya hukum-hukum yang ada masih dianggap belum memadai dan tidak diperbaharui terhadap tantangan dari penggunaan data yang bersifat modern. Pembaharuan terhadap hukum harus selalu dilakukan untuk menghadapi tantangan yang terus muncul (Privacy International, 2019, hal. 4).

Hal lain, yang perlu diperhatikan Indonesia, adanya *General Data Protection Regulation* (GDPR) yang memiliki pengaruh ekstrateritorial terhadap perusahaan yang memengaruhi data pribadi masyarakat Eropa. Hal ini dapat memengaruhi berbagai perusahaan luar negeri non-Eropa, termasuk perusahaan Indonesia dalam menjalankan kegiatan bisnisnya di Eropa.

Perlindungan Data di Indonesia

Hasani & Dehghantanha (2011) , Kebijakan perlindungan data seharusnya dapat mengontrol pengumpulan, penyimpanan dan penggunaan dari data pribadi untuk pihak manapun. Sehingga privasi dari ebrbagai individu seharusnya dapat dijamin oleh kerangka peraturan yang digunakan untuk mengurus dan mengolah data pribadi. Kebijakan ini (data protection act), dapat diaplikasikan kepada berbagai informasi atau opini yang diproses secara online maupun offline. Dalam hal ini informasi yang berhubungan dengan kebijakan, merupakan data yang berkaitan dengan individu baik hidup maupun sudah meninggal, serta berasal dari identitas individu yang telah jelas. User (Pengguna) akan menggunakan kebijakan ini untuk data subjects. Data subjects merupakan individu yang menjadi subjek dari data pribadi. Sementara pengguna data merupakan individu atau organisasi yang dapat mengontrol pengumpulan, penyimpandan, pemrosesan atau penggunaan dari berbagai jenis data pribadi (Lubis & Zulhuda, 2013).

Data protection secara eksplisit melindungi hal yang tidak menjadi bagian utama dari privasi, seperti the requirement of fair processing, consent, legitiamsi dan non-diskriminasi. Hal ini membuat konsep data protection sangat berhubungan dengan hak untuk menghargai privasi dan kehidupan keluarga. Pergerakan lintas batas data telah membuat berbagai hal dalam pemanfaatan internet mungkin untuk dilakukan, seperti mengupdate status facebook hingga melakukan transfer bank. Potensi pemanfaatan internet ini telah dianggap penting, sehingga menjadi salah satu pertimbangan bagi rezim internasional, yaitu Trans-Pacific Partnership yang mengintegrasikan hal tersebut ke dalam pengaturan e-commerce, layanan jasa keuangan, kekayaan intelektual dan telekomunikasi (Klein, 2015).

Pemilik Data Pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu.Setiap Penyelenggara Sistem Elektronik harus mempunyai aturan internal

perlindungan Data Pribadi untuk melaksanakan proses.Setiap Penyelenggara Sistem Elektronik harus menyusun aturan internal perlindungan Data Pribadi sebagai bentuk tindakan pencegahan untuk menghindari terjadinya kegagalan dalam perlindungan Data Pribadi yang dikelolanya. Perolehan dan pengumpulan Data Pribadi oleh Penyelenggara Sistem Elektronik wajib didasarkan kepada persetujuan atau berdasarkan ketentuan peraturan perundang-undangan. Data Pribadi yang disimpan dalam Sistem Elektronik merupakan jenis data yang telah diverifikasi keakuratannya dan telah dalam bentuk terenkripsi.

Data Pribadi wajib disimpan dalam Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan yang mengatur kewajiban jangka waktu penyimpanan Data Pribadi pada masing-masing Instansi Pengawas dan Pengatur Sektor atau paling singkat lima tahun, jika belum terdapat ketentuan peraturan perundang-undangan yang secara khusus mengatur untuk itu.Aturan data center.Keamanan data pribadi yang disimpat harus mengikuti ketentuan Pusat data(data center) dan pusat pemulihan bencana (disaster recovery center) Penyelenggara Sistem Elektronik untuk pelayanan publik yang digunakan untuk proses perlindungan wajib ditempatkan dalam wilayah negara Republik Indonesia.

Dalam aturan ini ditegaskan sistem elektronik yang dapat digunakan dalam proses perlindungan data pribadi adalah sistem elektronik yang sudah tersertifikasi dan mempunyai aturan internal tentang perlindungan data pribadi yang wajib memperhatikan aspek penerapan teknologi, sumber daya manusia, metode, dan biayanya. Pemilik data pribadi, berhak atas kerahasiaan data miliknya; berhak mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi; berhak mendapatkan akses untuk memperoleh historis data pribadinya; dan berhak meminta pemusnahan data perseorangan tertentu miliknya dalam sistem elektronik(Indotelko, 2016).

Gambar 1. Persebaran Hukum Privasi di Dunia 2018

Source: Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (January 25, 2018). Available at SSRN: <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

Dalam: Privacy International, The Keys to Data Protection, 2019:17

Jumlah data yang diproduksi telah mengalami perkembangan yang signifikan karena mengikuti perkembangan teknologi yang pesat, hal tersebut termasuk cara profiling dan tracking dan kecerdasan buatan. Perkembangan teknologi yang pesat ini akan membuat keberadaan hukum yang berlaku di berbagai negara dalam kondisi yang belum diperbaharui, terutama dalam hal melihat potensi data baru yang telah dicerna dalam industri dan system pemerintahan.

Terlebih dengan keberadaan 90% data yang ada di dunia merupakan data yang tercipta dalam dua tahun terakhir. Maka merupakan hal yang wajar apabila berbagai hukum yang berkaitan dengan data pribadi yang dibuat sebelum kemunculan perusahaan teknologi berpengaruh (Google, Facebook, Amazon dsb.) merupakan hukum yang tidak memadai. Kerangka perlindungan yang ada, biasanya memiliki keterbatasan. Namun, berbagai peraturan yang memiliki keterbatasan ini merupakan titik awal untuk memastikan peraturan dan hukum yang kuat untuk mengimplementasikan perlindungan data pribadi.

Keberadaan kerangka perlindungan data dapat memajukan individu, menghalangi praktik perusakan data dan membatasi eksploitasi data. Kerangka perlindungan juga dapat memberikan kerangka pengelolaan

secara nasional dan global untuk memastikan individu memiliki jaminan terhadap hak data yang mereka miliki. Para pihak yang memiliki kuasa untuk memproses data pribadi (dalam sector public dan privat) juga harus menuruti kewajiban dari hukum yang berlaku dan penegakan hukum yang kuat dapat digunakan terhadap orang-orang yang melanggar kewajiban dan perlindungan tersebut (Privacy International, 2019, hal. 10)

PEMBAHASAN

Penilaian terhadap komitmen Indonesia dalam mengelola keamanan data, dapat dikaitkan dengan penilaian yang telah dilakukan oleh International Telecommunication Union (ITU) dalam laporannya yang berjudul Global Security Index tahun 2017. Dalam laporan ini Indonesia termasuk dalam kategori maturing. Yaitu negara yang telah dianggap mengembangkan komitmen yang kompleks dan telah berpartisipasi dalam program dan inisiasi Cybersecurity (International Telecommunication Union, 2017, hal. 13).

Kaitan antara kejelasan posisi perusahaan pengelola data yang mengelola data dalam otomatis ataupun penyimpanan data dalam structured filing system yang berkaitan dengan individu. Perlindungan data yang dilakukan harus mengutamakan hak dasar yang dimiliki oleh individu, yaitu menyediakan akses terhadap para individu untuk mengakses data yang mereka miliki dan membentuk system akuntabilitas dan kewajiban yang jelas bagi para perusahaan yang memproses data (Privacy International, 2019, hal. 12).

Ruang Siber merupakan domain baru yang memerlukan tanggung jawab Bersama diantara para stakeholder di tingkat nasional dan global. Perlunya partisipasi dari berbagai pihak ini, berkaitan dengan adanya ratusan ribu alat yang tersambung, berupa computer, server, router, switches, yang ditopang oleh kabel serat optik yang memungkinkan infrastruktur nasional untuk bekerja. Ruang ini juga memungkinkan bagi terbentuknya borderless society, yang memberikan kesempatan bagi

meningkatkan kekayaan negara dan menstimulasi pertumbuhan ekonomi. Meskipun memberikan kesempatan bagi berbagai peluang, untuk menjaga ruang siber ini sangat diperlukan koordinasi berbagai stakeholder baik nasional maupun internasional yang terdiri dari pembuat kebijakan, penegak hukum, pemilik infrastruktur strategis, sektor swasta, organisasi keamanan nasional, para akademisi, administrasi public dan organisasi internasional. Stakeholder yang banyak merefleksikan dari sifat ruang siber sebagai jaringan global dan kepentingan dari semua negara (Nugraha, Roberts, Brown, & Sastrosubroto, 2016, hal. 8).

Dalam jangka waktu yang singkat, ruang siber yang semula dianggap sebagai domain yang netral, telah menjadi tempat bagi sasaran pengaruh inovasi teknologi dari Amerika Serikat ataupun negara lainnya. Domain ini telah menjadi tempat kompetisi diantara kelompok kepentingan, sekaligus tempat yang menjadi sasaran dari Invisible hand oleh pemerintah. Maka Ruang siber telah menjadi hal bagi target bagi persaingan, kolonisasi yang akan dipengaruhi oleh pemerintahan suatu negara, militer maupun korporasi swasta dan jaringan sipil (Choucri, 2012, hal. 8)

Konsep perlindungan data sering dianggap sebagai bagian dari perlindungan privasi. Hal tersebut sangat konsisten dengan pemahaman privasi sebagai bentuk dari kerahasiaan atau hak untuk menentang usaha pemberitahuan mengenai informasi yang disembunyikan atau hak untuk mengontrol informasi mengenai dirinya sendiri. Anmun, terdapat perbedaan diantara perlindungan data dengan perlindungan privasi, yaitu dalam hal scope, tujuan dan konten.

Ancaman Terhadap Data Pribadi di Indonesia

Sebagai bagian dari Kawasan Asia Tenggara, Indonesia diancam oleh potensi serangan siber sebagai target maupun launchpad oleh aktor anonym. Target serangan utama adalah

pencurian kekayaan intelektual dan informasi bisnis rahasia. Pemerintah dan korporasi menjadi pihak yang memiliki kendali untuk mengeloh data. Ancaman ini akan mengancam seluruh negara di dunai baik negara maju maupun berkembang (Direktur Jenderal Kerja Sama ASEAN, 2018, hal. 5).

Indonesia Bersama Malaysia dan Vietnam menjadi hotspot serangan siber. Indonesia yang menjadi target dan tempat bagi dilaksankannya serangan siber. (Direktur Jenderal Kerja Sama ASEAN, 2018, hal. 6). Ancaman ini akan terus mengganggu keamanan penggunaan internet, yang menjadi pendorong pertumbuhan ekonomi digital di Asia Tenggara. Terutama dengan adanya peluang investasi yang dapat menumbuhkan perusahaan teknologi (Direktur Jenderal Kerja Sama ASEAN, 2018, hal. 7).

Gambar 2 Persebaran Mobile Malware pada tahun 2018.

Sumber: Symantec, *Internet Security Threat Report Volume 24*, 2019:43

Kedaulatan Data dalam Keamanan Siber Indonesia

Keberadaan perusahaan teknologi multinasional seperti Google, Microsoft, Amazon, Yahoo, Alibaba dan sejenisnya yang menjadi data processor di Indonesia, merupakan perusahaan-perusahaan yang sampai saat ini belum membangun data server di Indonesia. Keberadaan data server di sebuah negara dapat memberikan dampak signifikan terhadap keamanan bagi negara dan warga

negara Indonesia. Hal tersebut dikarenakan data server menjadi tempat diolahnya arus data yang dikumpulkan oleh pengguna internet (Mercer, 2019). Di Negara yang mempraktikkan keamanan ketat seperti China, keberadaan data server dibangun untuk memenuhi tuntutan lokalisasi pengelolaan data, sehingga negara memiliki kekuasaan untuk mengontrol data yang tersimpan di server tersebut (China Briefing, 2017).

Penggunaan layanan komputasi awan telah memperluas partisipasi aktor dalam pemanfaatan ruang siber, serta memberikan ancaman terhadap kedaulatan negara. Dalam hal ini konsep data sovereignty, yaitu sebuah konsep yang menjelaskan informasi yang telah dikonversi dan disimpan dalam bentuk digital merupakan subjek bagi hukum yang berlaku di tempat data tersebut berada, dalam hal ini adalah data server. Polatin-Reuben dan Wright's (2014), menjelaskan data sovereignty sebagai kemampuan negara untuk mengontrol informasi yang diciptakan atau melewati wilayahnya, disertai adanya kekuasaan atau kapabilitas untuk melakukan pengontrolan. Komponen utama dari definisi ini adalah keinginan negara untuk melekatkan keterhubungan data dengan wilayah fisik, sebagai upaya untuk melindungi data dari pengawasan pihak asing (Baezner & Robin, 2018, hal. 31). Kehadiran sebuah data server di negara dapat menjadi bukti keterkaitan data dengan wilayah fisik yang menjadi bagian dari kedaulatan sebuah negara. Sehingga negara dapat bertindak apabila terdapat ancaman terhadap kedaulatan wilayahnya.

Pengadopsian layanan komputasi awan ini akan menimbulkan ancaman terhadap negara dengan penduduknya. Pertama, dalam penggunaan layanan. Pengguna tidak memiliki akses terhadap data pribadi yang dimiliki. Pengguna tidak memiliki kemampuan untuk mengawasi dan memengaruhi proses pengelolaan data. Hal ini terkait dengan sifat dari layanan komputasi awan yang melakukan transfer data diantara data server di berbagai negara. Hal ini menyebabkan data tersimpan di

berbagai negara yang dipilih oleh penyedia jasa (Sen, 2016, hal. 2).

Dalam perkembangan perekonomian digital yang terbaru, dapat dilihat kecenderungan bag perusahaan teknologi untuk melakukan ekspansi pelayanannya untuk menjangkau konsumen yang banyak (terutama dalam sektor e-commerce). Angka pengguna internet yang menjadi konsumen perusahaan penyedia jasa layanan sendiri akan terus meningkat.

Ancaman lain yang lebih besar karena tidak adanya data sovereignty ini, semakin penting ketika berbagai perusahaan teknologi multinasional yang beroperasi, masih memiliki keterhubungan erat dengan negara asal. Terutama apabila melihat kekuasaan yang dimiliki oleh aktor tersebut yang dapat memposisikan dirinya untuk menolak atau menghambat permintaan negara atau menjadi perpanjangan tangan negara dalam melakukan pengawasan di ruang siber. Posisi yang disebut sebagai "surveillance intermediaries", menurut Alan Rozenshtein akan menempatkan perusahaan teknologi sebagai bagian dari penegak hukum yang mengelola informasi pribadi yang dimiliki oleh publik (Harvard Law Review, 2019).

Peluang bagi terjadinya situasi yang membuat sebuah negara menjadi perpanjangan tangan negara induknya ini akan memberikan kerugian bagi Indonesia terkait dengan keamanan di dalam negeri. Terutama dengan berbagai isu penyadapan yang dilakukan oleh negara-negara yang memiliki kapabilitas spionase yang tinggi.

Tidak adanya control terhadap data-data yang diciptakan oleh penduduk Indonesia maupun data yang berkaitan akan menimbulkan Loss of integrity, lost of availability, lost of confidentiality dan Physical destruction. Loss of integrity merupakan kondisi dimana informasi yang ada dapat terdapat kondisi informasi yang ada dapat dimodifikasi secara tidak benar, Loss of availability merupakan kondisi dimana system informasi penting tidak bisa diakses oleh pengguna yang seharusnya memiliki otoritas,

Loss of confidentiality merupakan kondisi dimana informasi penting telah diakses oleh pengguna yang tidak memiliki wewenang dan Physical destruction merupakan kondisi dimana system informasi telah menciptakan malfungsi yang dampaknya dapat dirasakan secara fisik (Ahituv, 2009, hal. 15).

Hal tersebut membuat data yang dikoleksi oleh perusahaan asing di server luar negeri dapat dimanfaatkan secara bebas oleh perusahaan tersebut. Konsumen di Indonesia akan menemui kondisi dimana mereka sengaja atau tidak sengaja dikelabui untuk menyetujui pemanfaatan data pribadi dalam menggunakan layanan. Salah satu contoh dari permasalahan ini adalah *End User License-Agreement* (EULA) yang memberikan kesulitan terhadap pengguna biasa untuk membaca perjanjianⁱ.

Berbagai kasus yang menimbulkan tiga jenis ancaman tersebut, kemudian dapat dikaitkan dengan komponen Criticcal Infrastructure dalam Keamanan Siber, dimana Criticcal Infrastructure ini akan selalu menjadi target atau bagi para aktor lain. Posisi aspek ini sangat penting karena dapat memengaruhi ekonomi, penanggulangan bencana yang dapat mengancam keselamatan manusia (Betts & Sezer, 2014, hal. 2).

Di Indonesia, perlindungan terhadap infrastruktur masih dipengaruhi oleh prioritas keamanan negara yang terpaku pada permasalahan disinformasi, tanpa memberikan regulasi yang jelas terhadap pengumpulan dan pertukaran data pribadi yang dilakukan oleh perusahaan teknologi. Tanpa adanya pengendalian yang jelas akan muncul ancaman terhadap privasi.

Secara umum, Budi Rahardjo berpendapat pengelolaan ruang siber di Indonesia telah memberikan kesempatan yang aktif bagi berbagai pemain local untuk menjalankan kegiatannyaⁱⁱ.

Namun sebagai upaya untuk memberikan pelayanan yang luas dan menjangkau seluruh warga negara Indonesia, terdapat berbagai perusahaan asing yang memiliki jumlah pelanggan yang signifikan.

Dalam penyelenggaraan komunikasi dan internet provider terdapat perusahaan Indosat yang dimiliki oleh Ooredoo (Qatar) dan XL Axiata yang dimiliki oleh Group Axiata (Malaysia), 3 yang dimiliki oleh Hutchinson Holding (Hong Kong). Keberadaan berbagai perusahaan asing yang beroperasi dalam sektor teknologi ini telah mendapatkan izin dari Negara untuk bertindak sebagai perusahaan yang memberikan layanan. Pemerintah sendiri.

Dalam sektor perbankan, menurut Aidil Chendramata (Direktur Keamanan Informasi Kementerian Komunikasi dan Informatika), masih terdapat 10% perusahaan perbankan yang menyimpan data-data sensitive di luar negeri (Trisianty & Fauzi, 2017). Sektor perbankan ini menjadi target utama dari serangan siber. Serang siber di Indonesia di sektor perbankan. Pada mulanya berbentuk hacking. Namun terdapat peningkatan dalam bentuk ransomwareⁱⁱⁱ. Ancaman terhadap sektor ini akan lebih menargetkan keberadaan data yang dimiliki oleh penyedia layanan perbankan. Sehingga, sangat dibutuhkan sistem keamanan yang memiliki pelayanan yang memadai dan kredibilitas yang terjamin. Hal tersebut dapat dipenuhi oleh penyedia layanan komputasi awan yang memiliki infrastruktur dan pengalaman yang memadai.

Dampak terhadap Vital Core

Kondisi ketergantungan negara Indonesia terhadap berbagai perusahaan asing tersebut akan menemui permasalahan ketika terjadi kelalaian dalam pengelolaan sehingga menyebabkan terjadinya kebocoran data. Keberadaan data yang ada di berbagai sektor kehidupan akan memengaruhi perlindungan privasi. Data-data ini terdapat dalam berbagai sektor dan saling memengaruhi satu sama lain karena informasi yang dikumpulkan berkaitan dengan rekam jejak individu seseorangⁱⁱⁱ.

Pemerintah telah melakukan kebijakan yang memprioritaskan perlindungan kepada sektor ekonomi bagian finansial yang sangat dipegaruhi dalam perekonomian digital. Dalam Sektor ini Bank Indonesia (BI) dan

Otoritas Jasa Keuangan (OJK) telah memiliki upaya perlindungan risiko yang ketat untuk melindungi data-data yang bersifat strategis, termasuk data nasabah bank. Perlindungan tersebut terimplementasikan melalui adanya perangkat khusus seperti Direktur, tim audit dan tim forensic khusus yang menangani permasalahan tersebut. Tanggung jawab bank terhadap keamanan nasabahnya termasuk dalam kasus kebocoran data nasabah. Dalam hal ini bank memiliki tanggung jawab untuk menanggung kerugian dalam hal tanggung jawab sosialisasi dan menanggung biaya peradilanⁱ.

Untuk menangani ancaman kebocoran data, Pemerintah telah mempersiapkan pengelolaan keuangan melalui OJK dan BI untuk mengawal perlindungan data-data sensitive. Namun, perlindungan terhadap data yang dimiliki oleh pemilik kartu kredit dan database consumer masih bisa didapatkan secara dengan mudah. Bank-Bank yang ada di Indonesia tidak dapat melakukan perlindungan terhadap hal tersebut, karena tidak memiliki kewajiban hukum. Alasannya pembeli dari database konsumen ini bukanlah pegawai bank. Permasalahan ini harus ditangani oleh pemerintah agar perlindungan terhadap privasi warga negara Indonesia tetap terjaga (Palupy, 2011, hal. 45).

Konsep pengelolaan data pribadi, orang bisa, atau perusahaan boleh merekam data pribadi. Tetapi perusahaan tersebut harus memberitahu kepada pelanggan. Kedua, perusahaan itu hanya boleh memanfaatkan data pribadi untuk kepentingan yang sudah dijelaskan sebelumnya, yaitu yang tertera di EULA. Sehingga, secara idealnya tidak terjadi penjualan data pribadi tanpa sepengetahuan pemilik data.

Namun dalam praktiknya, terutama di industri asuransi (yang didominasi oleh perusahaan asing) konsumen selalu dihadapkan dalam bentuk kontrak baku, yaitu hanya bisa yes atau no ataupun jenis lainnya. Dalam hal ini masih terdapat Lembaga Otoritas Jasa Keuangan (OJK) yang masih

memberikan perlindungan. Namun, perlindungan ini belum memberikan keamanan yang memadai terhadap para konsumen di Indonesia yang menggunakan jasa perusahaan teknologi. Kontrak perusahaan teknologi asing seperti Grab melalui layanan uang elektroniknya. Dalam penggunaan kontrak jenis EULA (*End User License Agreement*) memberikan peluang bagi perusahaan untuk mengubah kontrak tanpa sepengetahuan konsumen. Praktik pengubahan EULA ini bahkan secara eksplisit juga dilakukan oleh Telkomsel. Tindakan ini merupakan pelanggaran terhadap Undang-Undang Perlindungan Konsumenⁱⁱⁱ.

Kebebasan perusahaan teknologi asing dalam mengkoleksi dan memanfaatkan data pribadi menempatkan individu dalam kondisi yang rentan. Meskipun terdapat standar praktik dalam pengelolaan data yang dianut oleh berbagai perusahaan tersebut, terutama dengan populernya teknik enkripsi, selalu terdapat celah yang mengkompromisasi privasi individu

Dalam menciptakan kondisi yang memberikan kebebasan dan kerahasiaan bagi para individu dan aktor lain agar bisa menjadi agent of change. Harus terapat anonimisasi dalam pemrosesan data pribadi. Melalui tehnik anonimisasi, yaitu: randomisasi, generalisasi dan pseudonimisasi. Berbagai pihak yang menjadi data processor diwajibkan untuk mencegah terjadinya identifikasi (terutama identifikasi secara personal) secara mudah dan mendalam untuk mencegah eksploitasi data (Working Party, 2014, hal. 3).

Bagi individu yang tidak memiliki pengetahuan terhadap berbagai tehnik security, encryption, keamanan data dan sejenisnya, maupun yang tidak bisa memanfaatkan software open-source. Akan menjadi individu yang rentan terhadap ancaman keamanan^{iv}.

Sementara negara sendiri dapat menjadi ancaman. Hal ini terkait dengan penempatan keamanan negara yang mendahului kepentingan individu atau penduduknya.

Negara dapat menjadi sumber ancaman terhadap keamanan pribadi warga Indonesia. Perusahaan keamanan asing secara tidak langsung ikut berpartisipasi dalam upaya melakukan pengawasan yang dapat mengganggu privasi penduduk Indonesia.

Hal tersebut kerja sama Pemerintah dengan Perusahaan keamanan luar negeri untuk memperkuat system keamanan justru memberikan alat bagi pemerintah untuk melakukan pengawasan yang dapat melanggar hak asasi yang seharusnya dimiliki oleh warga negara. Dalam hal ini teknologi pengawasan didapatkan dari kerja sama luar negeri.

Indonesia telah mengimpor IMSI Grabber teknologi dari sebuah perusahaan Inggris. Peralatan yang disebut dengan IMSI Catcher ini, sebenarnya merupakan teknologi yang dilisensi di Swiss. Peralatan ini dapat melakukan penyamaran sebagai salah satu operator seluler dan meminta pengguna untuk menyerahkan identitas pribadi seperti nomor kartu SIM. Dalam perkembangannya, IMSI Catcher ini dapat melakukan penyadapan suara, SMS dan data. Selain itu Indonesia juga pernah melakukan pembelian terhadap berbagai peralatan penyadapan mutakhir dari perusahaan Gamma TSE sebesar \$6,7 juta dollar. Sebagai bagian dari program pemerintah untuk memodernisasi alur sistem. Berbagai pembelian peralatan ini dapat menjadi ancaman terhadap penduduk Indonesia mengingat belum adanya peraturan komprehensif yang mengatur mengenai penyadapan yang menggunakan peralatan jenis tersebut, yang dapat melindungi hak asasi manusia (ELSAM & Privacy International, 2016, hal. 5) .

KESIMPULAN

Tidak adanya peraturan yang komprehensif untuk melindungi berbagai jenis data pribadi, membuat berbagai perusahaan teknologi asing dapat melakukan eksploitasi data secara bebas. Hal ini terjadi karena tidak adanya sanksi yang mengatur hubungan diantara negara dengan perusahaan asing. Sehingga, negara tidak

dapat mengatur pengolahan data yang ada di luar negeri. Keberadaan data server di luar negeri ini, menjadi penyebab Indonesia tidak bisa menerapkan *data sovereignty* terhadap data pribadi yang dikumpulkan dari penduduk Indonesia.

Ancaman yang dihadapi oleh masyarakat Indonesia tidak hanya berasal dari Perusahaan teknologi asing, tetapi juga dengan berasal dari pengelolaan yang salah dari pemerintah, seperti dalam pengelolaan identifikasi SIM Card. Meskipun pemerintah telah memiliki upaya untuk meningkatkan perlindungan melalui program Government Secure Intranet System. Namun, karena system ini belum selesai. Data-data penting kependudukan di lembaga-lembaga pemerintah masih mendapat ancaman dari serangan siber. Sehingga, privasi dari penduduk Indonesia masih dapat terkeksplotasi dan hal tersebut mengancam vital core dari penduduk Indonesia.

DAFTAR PUSTAKA

- Ahituv, N. (2009). *Modelling Cyber Security: Approaches, Methodology, Strategies*. In U. Gori. Washington DC: IOS Press.
- Akamai Technologies. (2014). *Akamai's [state of internet]* (Vol. 6). Akamai Technologies.
- Alkire, S. (2003). *A Conceptual Framework for Human Security*. Oxford: Centre for Research on Inequality, Human Security and Ethnicity, CRISE.
- Baezner, M., & Robin, P. (2018). *Trend Analysis: Cyber Sovereignty and Data Sovereignty*. Zürich: Center for Security Studies (CSS).
- Betts, J., & Sezer, S. (2014). *Ethics and Privacy in National Security and Critical Infrastructure Protection*. School of EEECS Queen University Belfast.
- Betz, D. J., & Stevens, T. (2011). *Cyberspace and The State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge.
- Buzan, B. (1983). *People, States and Fear*. Sussex: Wheatsheaf Book.

- Buzan, B. (2004). A Reductionist, Idealistic Notion that Adds Little Analytical Value. *Security Dialogue*, 369-370.
- China Briefing. (2017, Juli 26). *Establishing a Data Center in China*. Diakses pada Mei 14, 2019, dari china-briefing.com: <https://www.china-briefing.com/news/setting-shop-guide-chinas-data-centers/>
- Choucri, N. (2013, Oktober 13-15). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences. *Explorations in Cyber International Relations*. Massachusetts Institute of Technology.
- Direktur Jenderal Kerja Sama ASEAN. (2018, Agustus). ASEAN GOES DIGITAL. *Masyarakat ASEAN*.
- Elias, J., & Sutch, P. (2007). *International Relations: The Basic* (Vol. III). New York, New York: Routledge.
- ELSAM & Privacy International. (2016). The Right to Privacy in the Indonesia. *Stakeholder Report Universal Periodic Review : 27 th Session – Indonesia*, (hal. 9).
- Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. Congressional Research Service.
- Friedman, T. L. (2005, April 3). *It's a Flat World, After All*. Diakses pada September 15, 2018, dari nytimes.com: <https://www.nytimes.com/2005/04/03/magazine/its-a-flat-world-after-all.html>
- Gaspar, D., & Gómez, O. A. (2015). Human Security Thinking in Practice - 'Personal Security', 'Citizen Security', Comprehensive Mappings. *Contemporary Politics*.
- Hampson, F. O., Daudelin, J., Hay, J., Reid, H., & Martin, T. (2002). *Madness in the Multitude: Human Security and World Disorder*. Don Mills: Oxford University Press Canada.
- Harvard Law Review. (2019, Maret 14). *Harvard Law Review*. Diakses pada Mei 13, 2019, dari harvardlawreview.org: <https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/>
- Indotelko. (29 Desember 2016). *Indonesia sudah miliki aturan soal perlindungan Data Pribadi*. Diakses pada 13 April 2019 dari indotelko.com: <https://www.indotelko.com/kanal?c=id&it=indonesia-perindungan-data-pribadi>
- International Telecommunication Union. (2017). *Global Security Index 2017*. International Telecommunication Union.
- Johns, L. (2014, Juli 5). Evaluation of the Concept of Human Security. Diakses pada 24 September 2018, dari e-ir.com: <https://www.e-ir.info/2014/07/05/a-critical-evaluation-of-the-concept-of-human-security/>
- Klein, S. (23 November 2015). *The Data Is in the Details: Cross-Border Data Flows and the Trans-Pacific Partnership*. Diakses pada 25 Desember 2018, dari thediplomat.com: <https://thediplomat.com/2015/11/the-data-is-in-the-details-cross-border-data-flows-and-the-trans-pacific-partnership/>
- Lubis, M., & Zulhuda, S. (2013). A guideline to Enforce Privacy and Data Protection Regulation in Indonesia. *South East Asia journal of Contemporary Business, Economic and Law*, 2(3), 56-63.
- M.Shaw, T., J.MacLean, S., & R.Black, D. (2006). Introduction: A Decade of Human Security: What Prospects for Global Governance and New Multilateralisms. In T. M.Shaw, S. J.MacLean, & D. R.Black, *A Decade of Human Security : Global Governance and New Multilateralisms* (hal. 3-18). Burlington: Ashgate.
- Martin, M., & Owen, T. (2014). Introduction. In M. Martin, T. owen, M. Martin, & T. owen (Eds.), *Routledge Handbook of Human Security* (hal. 1- 13). New York: Routledge.
- McGrew, A. (2014). Globalization and global politics. In J. Baylis, S. Smith, & P. Owens, *The Globalizatio of World Politics : An introduction to international relations*.

- Mercer, E. (2019). *What is an Internet Data Center Server & How Does It Work?*. Diakses pada 13 Mei 2019, dari chron.com:
<https://smallbusiness.chron.com/internet-data-center-server-work-60422.html>
- Nugraha, Y., Roberts, T., Brown, I., & Sastrosubroto, A. S. (2016). *The Future of Cyber Security Capacity in Indonesia*. The University of Oxford for the Oxford Internet Institute.
- Palupy, H. E. (2011). *PRIVACY AND DATA PROTECTION : INDONESIA LEGAL*. Tilburg.
- Privacy International. (2019). *A Guide for Policy Engagement: The Keys to Data*. Privacy International. Diunduh dari <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>
- Rudiantara. (22 Januari 2016). Ketika UU ITE Menjadi Momok Masyarakat. Dipetik from tirto.id: <https://tirto.id/ketika-uu-ite-menjadi-momok-masyarakat-ct>.
- Schünemann, W. J., & Baumann, M.-O. (2017). *Privacy, Data Protection and Cybersecurity*. Springer.
- Sen, J. (2016). *Security and Privacy Issues in Cloud Computing*. NHSM Knowledge Campus.
- Shinoda, H. (2004). The Concept of Human Security: Historical and Theoretical Implications. *IPSHU English Research Report Series No. 19*, 5-22.
- Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar : What Everyone Needs to Know?* New York: Oxford University Press.
- Tadjabakhsh, S., & Chenoy, A. M. (2007). *Human Security : Concept and implications*. New York: Routledge.
- Trisianty, D., & Fauzi, M. (14 November 2017). *Penempatan Server di Dalam Negeri Jamin Kedaulatan Data*. Diakses pada 14 April 2019, from validnews.co:
<https://www.validnews.id/upper?q=LIMBUNG%20BERDAULAT%20DI%20DUNIA%20MAYA>
- W.Creswell, J. (2009). *Research design: qualitative, quantitative, and mixed methods*. Los Angeles: Sage.
- Waters, M. (1995). *Globalization* (II ed.). New York: Routledge.
- Working Party. (2014). *Opinion 05/2014 on Anonymisation Techniques*. Diunduh dari <https://www.pdpjournals.com/docs/88197.pdf>
-
- ^I Berdasarkan wawancara dengan Satriyo Wibowo selaku konsultan di Kementerian Komunikasi dan Informatika pada 13 Februari 2019.
-
- ^{II} Berdasarkan wawancara dengan Slamet Budihardjo selaku ketua ID-CERT pada 14 Februari 2019.
- ^{III} Berdasarkan wawancara dengan Ashwin Sastrosubroto selaku Dirjen Aplikasi Informatika Kementerian Komunikasi dan Informasi pada 6 Mei 2019.
- ^{IV} Berdasarkan korespondensi melalui email dengan Onno W. Purbo selaku Dosen Universitas Fakultas Ilmu Institut Informatika dan Bisnis Darmajaya. pada 9 Februari 2019.

BIOGRAFI

Wisnu Handi Prabowo adalah mahasiswa Program Studi Hubungan Internasional, fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran angkatan 2015. Memiliki ketertarikan (*area of interest*) dalam mempelajari pengaruh keamanan siber terhadap keamanan non-tradisional.

Satriya Wibawa adalah dosen Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran. Memiliki ketertarikan dalam mengkaji Keamanan Non-tradisional.

Fuad Azmi adalah dosen Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran. Memiliki ketertarikan dalam mengkaji Ekonomi Politik Global