Peperangan Asimetris
Volume 9, Nomor 2, 2023 E-ISSN 2830-0475

PENGAMANAN *BIG DATA* PADA OPERASI INFORMASI DALAM RANGKA MENINGKATKAN PERTUMBUHAN EKONOMI DIGITAL

ANDY NUR HIDAYAT, BASTARI, BAMBANG KUSTIAWAN
Universitas Pertahanan RI
Program Studi: Strategi Pertahanan Udara
e-mail: cackger@yahoo.co.id, bastari.rajatihang@idu.ac.id, bkustiawan168@gmail.com

Abstract

This paper describes the analysis of security vulnerabilities in the national defense system, especially in the cyber sector, related to the revision of PP 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PSTE) to PP 71 of 2019. The polemic arising from the revision is the change in the rules for placing data centers or big data infrastructure that originally had to be placed in the territory of the Republic of Indonesia has become a recommendation only. Thus, there are new opportunities for state actors or not state actors to use them as intentions and additional possible ways of acting to attack Indonesian defense. The analysis is carried out by means of a literature study and interviews with relevant stakeholders to obtain the latest data and factual information. From this study, it was found that the security gap due to the change in PP 82 of 2001 to PP 71 of 2019 must be anticipated properly, state sovereignty over the data of its citizens is reduced so that cooperation is needed to anticipate these changes between all stakeholders in Indonesia. Furthermore, the rules for placing data centers can be reviewed so that data problems in cyber warfare can be anticipated properly by the TNI.

Key words *: big data, data center, PP 71 of 2019, cyberwarfare, data sovereignty*

1. Pendahuluan

Kehidupan di era 4.0 sangat bergantung pada kecerdasan artifisial, *cloud systems, smart city, internet of things* dan *big data*. Kemampuan *hardware* harus dapat mengimbangi tuntutan perkembangan zaman tersebut. Salah satu *hardware* pendukung adalah *data center* dan *data recovery center* untuk seluruh layanan tersebut atau yang

lebih dikenal dengan infrastruktur *big data. Big data* sendiri merupakan data dengan volume yang sangat besar hingga ukuran zettabytes, keragaman data yang disimpan dapat terstruktur sampai acak, kecepatan proses data yang sangat cepat dari bermacam sumber hingga kondisi *real time*, *veracity* (kebenaran) data yang tidak perlu diragukan dan nilai manfaat dari seluruh data yang disimpan (Demechenko, 2014). Pendeknya *big data* dapat menggantikan database konvensional jika pengguna butuh layanan data yg sedemikian besar, perlu sedemikian cepat dan perlu pemrosesan yang sedemikian *powerfull* (*too big, too fast, too hard)* (Madden:2012). Dimasa mendatang *big data* digunakan sebagai *personalized service* dalam bekerja, sebagai bagian *internet security*, sebagai data pengobatan individu, dan berbagai kebutuhan manusia modern lainnya (Jianqing, 2014). Kejahatan media siber muncul karena berbagai macam sebab antara lain lebih murah, lebih rahasia, target yang lebih besar, dampak yang luas dan dapat dilaksanakan dengan berpindah tempat. Upaya untuk menangkal kejahatan siber yaitu melalui pengendalian informasi komunikasi dan identifikasi aktifitas internet menjadi semakin sulit (Fitriana dkk, 2017).

Tantangan pemerintah dalam issue keamanan *big data* di Indonesia tergantung pada data, teknologi, proses dan Sumber Daya Manusia (SDM)(Aryasa, 2015). Perlindungan hukum pada *big data* merupakan suatu keharusan terhadap penyalahgunaan informasi data baik milik individu, organisasi ataupun data milik negara. Sehingga, Kedaulatan *big data* menjadi hal yang mutlak (Rohendi, 2020).

Data yang bocor ke tangan musuh dipastikan merupakan suatu ancaman ditambah lagi dengan keberadaan infrastruktur yang berada di luar yuridiksi nasional keadaan tersebut semakin bertambah kompleks. Tantangan perang asimetrik dalam kejahatan internasional intensitasnya semakin tinggi yaitu *Composite assymetri* akan semakin susah untuk dijawab jika kemampuan pertahanan siber paling dasar belum dimiliki (Anggoro,2011).

Dalam menghadapi kemungkinan perang modern, TNI harus mengantisipasi dan menutup celah musuh untuk menyerang berupa kemungkinan cara bertindak. Pada

prakteknya, langkah penanganan *cyberspace* tidak akan sama penanganannya dengan penanganan di dunia nyata (Lubis, 2017). Kemudian, standarisasi pemerintah dalam integrasi data dapat digunakan sebagai aturan pemanfaatan *big data* di Indonesia, disamping ketersediaan data, keamanan data dan infrastruktur penunjang dapat digunakan sebagai instrumen lanjutan (Nugroho dkk,2019).

Untuk mengatur penyediaan, penggunaan dan penyelenggaraan transaksi elektronik dan sebagai turunan dari Undang-undang ITE No 11 tahun 2008, pemerintah mengeluarkan PP 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Seiring berjalannya waktu, aturan tersebut direvisi dengan salah satu pertimbangan bahwa kewajiban membangun infrastruktur *big data* dapat merusak iklim investasi. Hasil dari revisi PP 82 tahun 2012 telah ditetapkan pemerintah ke dalam PP 71 tahun 2019. Menanggapi revisi tersebut sebagian kalangan menyebutkan tidak tepat karena dipandang dari segi bisnis tidak menciptakan kepastian iklim investasi, berat sebelah dan lebih banyak lagi argumen yang lain. Data yang disajikan oleh Asosiasi Big Data dan AI (ABDI) menyatakan bahwa petinggi Amazon akan berinvestasi dengan nilai hampir Rp. 14 trilliun dalam kurun waktu 10 tahun. Hal tersebut sebagai salah satu sanggahan yang nyata, bahwa alasan pemerintah dalam melaksanakan revisi untuk meningkatkan iklim investasi kurang tepat.

Dari kacamata pertahanan dan antisipasi perang modern hal tersebut adalah celah yang lumayan lebar. *Big data* yang saat ini lebih berharga dari minyak bumi adalah salah satu komponen penting dalam *cyberwarfare.* Dari kharakteristik tersebut, tentunya *Cyberwarfare* dapat menggunakan *big data* sebagai alat, sebagai sumber dan sebagai target serangan pada perang modern seperti saat sekarang ini (Berson, 2011). Kita dapat mengibaratkan *big data* sebagai uang dalam jumlah besar. Usaha kita menyimpan uang tersebut dengan membeli sebuah brankas, namun brankas tersebut kita taruh di tetangga kita, bukan di rumah sendiri. Jadi, bisa dibayangkan ancaman yang sungguh nyata bagi uang kita tersebut. Dalam bahasa lain, *big data* yang berada di wilayah

kedaulatan sendiri saja merupakan aset yang harus dilindungi yang rentan terhadap serangan *cyberwarfare,* apalagi jika berada di wilayah orang lain.

Hasil penelitian ini berupa rekomendasi konsep pengamanan *big data* yang dapat dijadikan pertimbangan seluruh *stake holder* untuk duduk bersama agar terjadi kesepahaman dalam mendukung perekonomian tanpa mengabaikan pertahanan nasional. Jika perlu, demi penguatan sistem pertahanan nasional, sekiranya pemerintah tidak perlu berat hati apalagi merasa terpaksa untuk mencabut revisi yang telah dikeluarkan tersebut. Dan tentu saja, media penelitian sebagai mimbar akademis ini tidak ada kepentingan lain, selain memunculkan sisi lain konsep bernegara dari sistem *big data.* Kajian yang mendalam lewat penelitian ini diharapkan menjadi penggugah rasa kebangsaan dan bernegara agar sistem pertahanan yang dibangun oleh seluruh komponen bangsa tidak sia-sia. Sehingga, rekomendasi dari tulisan ini nantinya tidak dipandang bertentangan dengan pemerintah melainkan sebagai bentuk kontribusi akademis dalam mewujudkan konsep keterpaduan pemerintah-universitas dan industri *(triple helix conceps).*

Rumusan permasalahan yang akan dibahas pada penelitian tesis ini adalah sebagai berikut :

Apakah latar belakang revisi PP 82 tahun 2012, aplikasi dan dampak pelaksanaannya dalam pengamanan *big data* bagi pemerintah, industri dan pertahanan nasional?

Mengapa Indonesia perlu mempersiapkan sumber daya untuk pertahanan nasional bidang siber khususnya pengamanan *big data* pada operasi informasi?

Bagaimana bentuk pengamanan *big data* dalam pertahanan nasional bidang siber pada operasi informasi akibat adanya revisi PP 82 tahun 2012?

2. Tinjauan Pustaka

Definisi *big data* menurut Glosarium IT Gartner adalah aset informasi bervolume tinggi, berkecepatan tinggi, dan beragam yang menuntut bentuk pemrosesan informasi

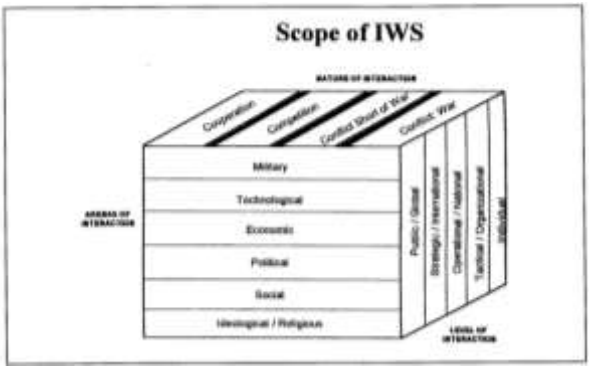
inovatif yang hemat biaya untuk meningkatkan wawasan dan pengambilan keputusan. Pada pengertian lain oleh *Tech America Foundation* mendefinisikan *big data* sebagai "tiga V", suatu istilah yang mendeskripsikan volume besar data berkecepatan tinggi, kompleks, dan variabel yang memerlukan teknik dan teknologi canggih untuk memungkinkan penangkapan, penyimpanan, distribusi, pengelolaan, dan analisis informasi. Dari dua pengertian tersebut terdapat benang merah yang hampir sama, yaitu volume besar, kecepatan tinggi, variabel yang kompleks. Sehingga, jika membicarakan *big data* tidak hanya besarnya kapasitas saja, melainkan tingkat kecepatan analisa yang tinggi meskipun data yang diolah mempunyai variabel yang kompleks.

Teori Manajemen Privasi Komunikasi *(CPM theory)* (Petronio, 2002) mengungkapkan dengan pasti bahwa otoritas untuk membagi informasi yang berisifat pribadi terletak di masing-masing individu berdasarkan pertimbangan yang bersifat subyektif juga. Informasi pribadi yang dibagikan ke ranah publik tersebut disaring oleh individu tanpa ada campur tangan orang lain. Enam prinsip dalam teori CPM tersebut adalah *Public-Private Dialectical Tension* (ketegangan dialektis publik-pribadi), *Private-Information* (informasi-pribadi), *Privacy Rules* (aturan privasi), *Boundaries* (batasan), *Boundary Coordination* (koordinasi batas), *Boundary Turbulence* (turbulensi batas).

Pengambilan data pada *big data* berbeda dengan pembagian informasi pribadi pada media sosial. Perlindungan data pribadi pada media sosial dilakukan pada saat pengambilan data, perlindungan pada saat penyimpanan dan proteksi saat pemrosesan data (Irwansyah, 2020). Sedangkan, *big data* dapat mengambil data secara acak melalui teknik *mining* yang bergerak cepat seiring perkembangan dan tuntutan kebutuhan (Bifet, 2013). Data yang terkumpul tidak memerlukan izin individu membagikan informasi apa pun. *Big data* mampu mendapatkan data dengan mudah melalui jaringan data yang digunakan pada suatu waktu tertentu bahkan lewat suatu halaman yang dikunjungi pada suatu *website.* Sehingga, teori CPM membutuhkan suatu regulasi yang kuat agar privasi individu tetap terjaga.

Operasi informasi merupakan jenis operasi yang baru diintensifkan pada saat perang Iraq yaitu Integrasi Operasi Informasi (Ops Info) selama *Operations Enduring Freedom* dan *Iraqi Freedom* (Cox, 2006) . Sebagian besar komandan pasukan Amerika menganggap Ops Info tidak efektif karena Ops Info tidak dapat beradaptasi terhadap lingkungan Afghanistan dan Irak yang kompleks. Kedua lokasi perang tersebut merupakan contoh yang baik dan contoh yang gagal bagaimana komandan mengintegrasikan Ops Info secara efektif. Ops Info sendiri merupakan bagian dari operasi besar yang bertujuan melindungi informasi sendiri dan mengungguli informasi lawan. Untuk mewujudkannya Ops Info harus mampu melindungi negara dalam hal penyimpanan data dengan menggunakan seluruh sistem operasi (*antivirus, firewall, gateway* dll) dan melindungi infrastruktur kritis data negara (Denning, 1998).

Perang informasi berubah sesuai dengan perkembangan zaman menyesuaikan teknologi informasi dan hal tersebut berpengaruh terhadap kemampuan dan strategi militer suatu negara (Alberts, 1998). Dimensi perang informasi terdiri dari tiga *scope* yaitu arena interaksi, level interaksi dan sifat interaksi dari pengguna informasi. Dan untuk mempertahankan seluruh dimensi yang ada dengan berbagai macam jenis serangan, negara harus mampu menagkal seragan terhadap infrastruktur informasi termasuk yang saat ini dikenal dengan "*hacker warfare*" dan "*digital warfare*". *Scope* dari Strategi dan Perang Informasi (IWS) dapat dilihat pada gambar 1.



Gambar 1 *Scope* IWS (albert,1998:3)

Pada gambar di atas diketahui bahwa *nation states* atau kombinasi dari *nation states* bukan satu-satunya pemain operasi innformasi. *Non-state actors* bermain pada bidang

politik, etnis sampai ideologi agama yang dimulai dari sekedar kerja sama, kompetisi namun bisa sampai konflik yang berupa perang. Level interaksi pada IWS cukup jauh rentangnya dari individu, organisasi, nasional, interasional sampai dengan global. Keseluruhan level interaksi, arena maupun kepentingan interaksi pada IWS dapat mengambil bagian dalam serangan informasi dan mengembangkan informasi strategis untuk kepentingannya masing-masing.

3. Metode Penelitian

Metode penelitian ini adalah dengan pendekatan Metode Kualitatif. Metode kualitatif merupakan metode yang digunakan untuk meneliti masalah sosial dengan menekankan wawancara dan relasi di dalamya (Easterberg, 1999). Pendekatan deskriptif kualitatif ini dipilih karena penulis ingin berfokus menggali informasi dari pemangku hajat *big data* dan melihat kondisi lapangan secara langsung dalam kaitannya dengan Operasi Udara untuk Perang (OMP) berupa Operasi Informasi.

Data yang digunakan pada penelitian ini terdiri atas :

a. Data primer penelitian ini diperoleh dengan melaksanakan wawancara langsung dan kunjungan lapangan. Wawancara dilaksanakan untuk mendapatkan informasi secara langsung dari pelaku langsung dan kunjungan lapangan bertujuan untuk melihat kondisi nyata didasarkan hasil wawancara dan literature yang telah ada.

b. Data sekunder penelitian ini digunakan sebagai pijakan teori berfikir berupa produk penelitian, buku, literatur dan paparan yang berhubungan dengan *big data* dan operasi informasi TNI AU.

4. Hasil dan Diskusi

4.1 Hasil

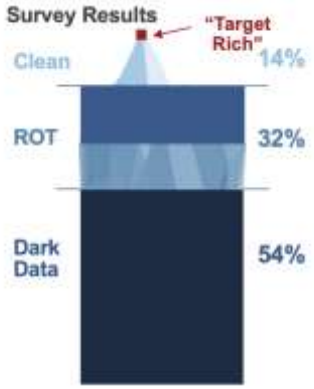
Perencanaan strategi pada operasi informasi mencakup semua sektor operasi. Perencanaan yang baik mampu mengetahui celah kekurangan yang mungkin terjadi di masa pelaksanaan mendatang (Jonni Mahroza et al.,2022). Revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 menciptakan lubang yang harus diantisipasi. Celah tersebut adalah pengaturan penempatan *data center* untuk PSE privat yang tidak wajib berada di wilayah kedaulatan sendiri sehingga proses pengamanan *hardware* dan kontennya semakin berat dilaksanakan.

Pemerintah Republik Indonesia telah menetapkan UU No 11 tahun 2008 tentang ITE dan UU No 19 Tahun 2016 sebagai perubahan pertama atas UU 11 Tahun 2008. Keberadaan Internet sebagai hasil dari revolusi industri 4.0 membutuhkan regulasi sebagai dasar operasional maupun hukum yang kuat dalam penindakan atas penyimpangan pelaksanaan agar diperoleh ketertiban dan keamanan atas individu maupun kepentingan umum.

Pemerintah menyadari bahwa Indonesia merupakan pasar yang besar internet. Revolusi industri 4.0 berkisar pada penggunaan *internet of things, big data, smart city, data clouds* dan *security systems* digunakan hampir 38,4% penduduk Indonesia pada tahun 2018 dan meningkat 8,9% menjadi 41,4% pada tahun 2019. Data yang sedemikian besar dan potensi pasar yang luar biasa membutuhkan regulasi yang *update* dan flexible dengan perubahan zaman. PP 82 tahun 2012 dianggap Kementrian Kominfo sudah waktunya dilaksanakan perubahan sehingga dilaksanakanlah proses Revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019.

Pemakaian internet disertai dengan penambangan data dilakukan oleh pihak pemilik aplikasi dan penyedia layanan publik meliputi perbankan, jasa, retail dan lain-lain. Data tidak terstruktur (*instructured data)* yang terkumpul mulai berbentuk eksponensial sejak tahun 2015. Pengumpulan data tersebut semakin mudah dianalisa dengan adanya *big data.* Data yang terkumpul tersebut dianalisa dan merupakan "produk mahal" di dunia saat ini. Pihak yang membutuhkan pemasaran produk, pabrik yang membutuhkan ekspansi pasar, industri yang memerlukan masukan selera

khalayak masyarakat merupakan pihak yang jamak membutuhkan hasil analisis *big data* dari *unstructured data.* Pelaksanaan analisis data dapat dilihat pada gambar 2.



Gambar 2. perbandingan analisis *unstructured data* (sumber ABDI, 2021)

Untuk menganalisis jutaan data tidak terstruktur menjadi informasi yang berguna sangat susah dan membutuhkan waktu yang tidak sebentar jika tidak menggunakan *big data*. *Dark data* merupakan bagian dari *data lake* (danau data) yang memerlukan analisis lebih dalam namun cenderung tidak terpakai. Hasil analisis *big data* yang terpakai menghasilkan ROT (Redundant, Obsolete, Trivial- not relevan) dan *clean data.* Persentase *clean data* yang digunakan sebagai target adalah kurang dari 15% dan hal terebut adalah hasil *mining data* yang sepadan dengan biaya yang dikeluarkan.

Big data sudah sedemikian menyatu dalam kehidupan saat ini. Pengguna internet tidak sadar bahwa dengan memakai internet, maka individu tersebut juga menggunakan layanan *big data* dari pemilik aplikasi yang digunakan. Pendapatan vendor *big data* semakin meningkat dari tahun ke tahun. Vendor tersebut bergerak dalam bidang *hardware, software, data base, data warehouse, consultant, sosial media, storage* dan terakhir adalah *e-commerce.* Pendapatan terbesar yang mempunyai perwakilan di regional ASEAN pada tahun 2013 adalah IBM sebagai layanan *hardware* sebesar 1.368 juta dollar amerika.

Mekanisme hukum untuk melindungi data pribadi tidak bisa dilaksanakan jika UU yang khusus mengatur perlinndungan data pribadi belum ada. Saat ini, Indonesia tidak termasuk 136 negara yang memiliki UU Perlindungan Data Pribadi (UU PDP)

(Bisnis Tempo, 30 Desember 2020). Pembahasan UU Perlindungan Data Pribadi sangat alot di legislatif dan menghabiskan waktu hampir 2(dua) tahun. Rancangan undang-undang yang nantinya ditetapkan juga harus memberikan efek jera. Hukuman bagi yang melanggar undang-undang tersebut bisa berupa pidana dan denda yang sangat besar. Proyeksi hukuman bisa melihat EUGDPR (*European General Data Protection Regulation)* yang memberikan denda sampai ratusan ribu euro jika penggunna data pribadi tidak bisa mengamankan data pribadi warga negara Uni Eropa. Dengan demikian, efek jera bagi personel atau korporasi pelanggar bisa diperoleh dan lebih *concern* dalam menyimpan dan menggunakan data pribadi.

UU Perlindungan Data Pribadi yang belum ditetapkan oleh pihak Legislatif Indonesia mengakibatkan badan atau organisasi yang melindungi data pribadi belum terbentuk di Indonesia. Dengan membentuk badan perlindungan pribadi, maka badan tersebut dapat mengadvokasi hak individu dalam keamanan data. Muaranya adalah warga negara merasa aman dan kehadiran negara dalam melindungi warga negara terpenuhi.

Pengguna internet dan aplikasi di internet belum sepenuhnya paham aturan yang berlaku dan syarat ketentuan penggunaan aplikasi. Di Indonesia kesadaran dalam membaca syarat dan ketentuan layanan sangat rendah. Beberapa aplikasi yang mengambil data privat milik pelanggan untuk kepentingan sepihak lumayan banyak terjadi. Pihak aplikasi kemudian membagikan data tersebut dengan pihak ketiga untuk ditawari produk-produk pihak ketiga tersebut. Hal ini dapat terjadi karena pengguna tidak menyadari pilihannya saat mengaktifkan aplikasi mempunyai dampak sedemikian besar.

Sosialisasi dari pemerintah perlu dilaksanakan dalam berbagai bentuk agar pengamanan data dari sisi pengguna dapat tercapai. Pemerintah bisa menggunakan iklan layanan masyarakat di televisi nasional, membuat banner secara masif di tempat-tempat strategis, koran nasional, membuat pesan melalui sms dan memberikan

pencerahan pada layanan media sosial. Dengan demikian, kesadaran masyarakat diharapkan dapat tumbuh dengan baik dalam mengamankan datannya sendiri.

Big data dengan *data center* dan *data recovery center* yang berada di Indonesia mempunyai banyak keuntungan. Pemanfaatan pusat data yang dekat dengan pengguna akan meningkatkan kecepatan akses dan biaya akses menjadi rendah (koran bisnis, 18 Juni 2021). Akses biaya rendah tersebut diperoleh dari jumlah lajur yang dilalui untuk mengakses pusat data. Koneksi internet ke luar negeri membutuhkan lebih banyak hop untuk melaksanakan satu *route* dibandingkan dengan koneksi di dalam negeri. Dengan banyaknya hop yang dilalui otomatis akses data yang dibutuhkan lebih banyak dan biaya yang dikeluarkan menjadi lebih besar.

Lebih jauh lagi pengguna akan merasa nyaman dalam menggunakan teknologi *internet of things* tersebut. Adanya revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 memberikan dampak yang signifikan. Pemerintah sebagai pemangku kebijakan mempunyai pertimbangan dalam mengambil langkah revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 dan Pemerintah mempunyai ekspektasi bahwa aturan yang direvisi tersebut akan membawa kesejahteraan untuk seluruh rakyat Indonesia.

Revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 berawal dari kata pelayanan publik pada pasal 17 ayat 2 PP 82 tahun 2012 yang mempunyai arti terlalu luas dan merupakan keberatan dari berbagai kalangan, bunyinya adalah sebagai berikut :

"Penyelenggara Sistem Elektronik untuk pelayanan publik wajib menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia untuk kepentingan penegakan hukum, perlindungan, dan penegakan kedaulatan negara terhadap data warga negaranya"

Kata publik menjadi keberatan pihak asing seperti Google yang menganggap penempatan *data center* tersebut memberatkan. Konsekuensi dari penempatan *data center* tidak hanya investasi infrastruktur, namun menambahkan kewajiban pertahun berupa pajak dan biaya perawatan. Pihak asosiasi penyedia *Big Data* di Indonesia

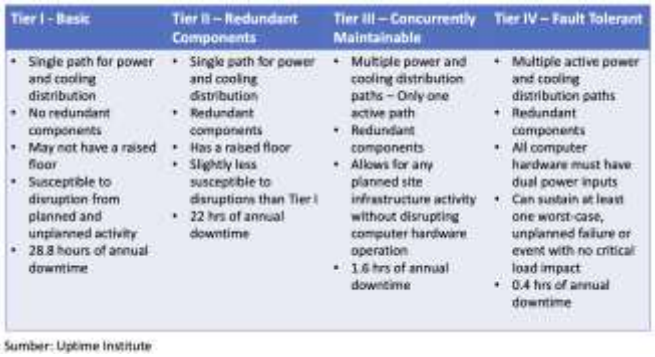
antara lain ASP, AJI, ACCI, ABDI pada dasarnya mendukung revisi penempatan *data center* dan *data recovery center* karena kata "pelayanan publik" yang harus menempatkan infrastrukturnya di Indonesia melemahkan, karena pelayanan privat menjadi terabaikan. ABDI mendukung revisi dengan pasal 17 tetap ada namun kata "publik" dihilangkan. Sehingga, seluruh *data center* dan *data recovery center* tidak memandan ranah publik dan privat semua wajib membangun infrastrukturnya di wilayah NKRI.

Dari pasal 17 ayat 2 tersebut, Penyelenggara sistem elektronik untuk pelayanan publik, wajib menempatkan *data center* dan *data recovery center* di wilayah Indonesia. Tujuannya adalah Untuk kepentingan penegakan hukum, perlindungan dan penegakan kedaulatan Negara terhadap data warga Negara itu sendiri. Adanya permasalahan mengenai kompleksitas Pelayanan Publik, membuat Pelayanan Publik ini dihubungkan dengan Undang-undang Pelayanan Publik No. 25 tahun 2009 dan hal tersebut lebih kearah Barang, Jasa dan Administratif. Barang, Jasa dan Administratif untuk Pelayanan Publik sehingga maknanya menjadi sangat sempit. ketidakjelasan mengenai Ruang Lingkup Pelayanan Publik ini perlu dijelaskan dengan rinci. Permasalahan selanjutnya adalah Multinational Companies dari luar negeri, seperti Google, Facebook, tidak bisa terjawab dengan jelas wajib memiliki Pusat Data di Indonesia pada PP 82 tahun 2012.

Penekanan layanan publik dari sisi perbankan dikuatkan dengan penekanan dari OJK (Otoritas Jasa Keuangan) yang berisi bahwa Perbankan wajib menempatkan Pusat Datanya di Indonesia. Pelaksanaan bidang lain diserahkan pada pemangku kepentingan di sector masing-masing.

Penyelenggaraan Sistem Elektronik (PSE) dibagi dalam PSE Lingkup Privat dan PSE Lingkup Publik dengan tujuan adalah agar masing-masing dari PSE itu bisa diidentifikasi dengan jelas. Pada PP 82 tahun 2012 pembangunan keamanan cyber belum dijelaskan dengan rinci baik PSE privat dan PSE public. Pemerintah berharap dengan revisi menjadi PP 71 tahun 2019 terdapat peran berbagai pihak dalam Pembangunan Ruang Cyber yang aman dan andal.

Bank Asing yang membuka cabang di Indonesia termasuk yang menolak membangun *data center* dan *data recovery center* di Indonesia. Alasan resmi mereka adalah Indonesia belum mendukung *tier IV* jika akan membangun *data center* dan *data recovery center.* Tier merupakan klasifikasi *data center* dan *data recovery center* dimana situs dapat mempertahankan setidaknya satu kegagalan infrastruktur terburuk yang tidak diperkirakan tanpa dampak beban kritis dan dianggap toleran terhadap kesalahan dalam cara kerjanya (Turner, 2001). Klasifikasi tier dapat dilihat pada gambar 3.



Tier I - Basic	Tier II – Redundant Components	Tier III – Concurrently Maintainable	Tier IV – Fault Tolerant
• Single path for power and cooling distribution • No redundant components • May not have a raised floor • Susceptible to disruption from planned and unplanned activity • 28.8 hours of annual downtime	• Single path for power and cooling distribution • Redundant components • Has a raised floor • Slightly less susceptible to disruptions than Tier I • 22 hrs of annual downtime	• Multiple power and cooling distribution paths – Only one active path • Redundant components • Allows for any planned site infrastructure activity without disrupting computer hardware operation • 1.6 hrs of annual downtime	• Multiple active power and cooling distribution paths • Redundant components • All computer hardware must have dual power inputs • Can sustain at least one worst-case, unplanned failure or event with no critical load impact • 0.4 hrs of annual downtime

Sumber: Uptime Institute

Gambar 3 *Tier Classifications*

Pada gambar 3 Tier I merupakan level basic dengan keandalan 99,671%. Pada level tersebut *annual downtime* (waktu tidak beroperasi) sekitar 28,8 jam setiap tahunnya. Tier II mempunyai keandalan sistem sebesar 99,741% dengan penambahan penambahan komponen dibandingkan Tier I. Tier III dan IV memiliki keandalan masing-masing 99,982% dan 99,995%. Pada Tier IV *downtime* nya hanya sekitar 0,4%.

Penjelasan Bank asing tersebut masuk dalam logika namun berkebalikan dengan kondisi faktual yaitu PT Telkom saat ini sudah memiliki infrastruktur *data center* dengan level Tier IV. Sebagian dari bank asing dan perusahaan asing yang berkeberatan dengan regulasi penempatan *big data* di Indonesia bahkan menggunakan diplomasi politik melalui kedutaan negara asal agar aturan tersebut dilonggarkan. Pada bagian lain perusahaan multinasional lainnya sangat mendukung regulasi PP 82 tahun 2012 untuk menempatkan *big data* di Indonesia, seperti Microsoft, IBM dan Dell. Permasalahan yang menjadi awal keberatan pihak asing adalah adanya konsekuensi pajak yang harus dibayar setiap tahunnya jika membangun *data center* dan *data recovery*

center di Indonesia. Perihal tersebut tentu saja tidak disampaikan secara langsung namun permasalahan pajak layanan sudah menjadi isu global di berbagai negara.

Proses revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 khususnya tentang penempatan pusat data menimbulkan kekhawatiran dari berbagai kalangan. Masukan dari kemenko Polhukam selaku *supervisi* dari Kementrian Informasi selaku regulator dari pelaksanaan PSE. Masukan agar revisi PP No 82/2012 dipertimbangkan salah satunya berasal dari Menteri Koordinator Bidang Politik, Hukum dan Keamanan Republik Indonesia (Menkopolhukam RI) melalui Surat Nomor B-23/KI.00.01/1/2019 tanggal 31 Januari 2019. Menkopolhukam RI mempunyai pandangan bahwa relaksasi terhadap infrastruktur big data dapat berdampak sistemik terhadap IPOLEKSOSBUDHANKAM Indonesia pada masa ekonomi data, karena Undang-Undang terhadap perlindungan data belum ada. Perlindungan data pribadi belum dibahas pada saat itu dan sampai sekarang masih tahap pembahasan. Sehingga bisa diketahui potensi ancaman terhadap data pribadi yang dikumpulkan oleh Pemerintah maupun Swasta.

4.2 Diskusi

Urgensi RPP No 82 tahun 2012 tidak mendesak untuk dilaksanakan revisi. Menkopolhukam RI menyatakan bahwa sistem keamanan siber nasional dalam proses menuju tata kelola dan aturan keamanan digital supaya kedaulatan siber RI terjaga. Wacana tersebut sangat realistis mengingat siber di Indonesia bagai hutan belantara, karena masyarakat tahunya adalah UU ITE tahun 2008 yang belum jelas objek hukumnya dan cenderung subjektif dalam pelaksanaannya. PP No 82 Tahun 2012 jelas sekali mewajibkan bahwa *data center* harus berada di wilayah NKRI, namun sampai dengan wacana revisi tahun 2019, sanksi hukum pelanggarannya belum pernah ada. Hal tersebut mestinya tidak terjadi dengan kurun waktu 7 (tujuh) tahun PP 82 tahun 2012 berlaku diundangkan jika turunannya berupa Peraturan Menteri Kemenkominfo dengan jelas mengatur sanksinya tersebut.

Pertimbangan paling penting dari Menkopulhukam RI adalah penegakan hukum yang akan mengalami kesulitan jika pihak Indonesia membutuhkan akses data sedangkan data tersebut berada di luar negeri. Ketentuan negara lain akan menghalangi proses tersebut ditambah potensi hilangnya *evidence* dari proses hukum tersebut.

Sumber daya pertahanan siber merupakan segenap kemampuan bangsa yang bisa dimanfaatkan dalam langkah nyata dalam pertahanan siber. Badan Siber dan Sandi Negara (BSSN) mempunyai tugas mengkonsolidasikan semua sumber daya di Indonesia terkait masalah keamanan siber. Era perang siber dan perang informasi tentu saja menggunakan media informasi sebagai senjata yang telah direkayasa. Rekayasa informasi memerlukan kejelian tingkat tinggi dan hal tersebut terbantu dengan adanya pemanfaatan *big data* dalam merumuskan ancaman dari musuh. Menurut Mc. Donell dan Sayers, Ancaman dari musuh dari bidang siber terdiri atas ancaman *hardware*, ancaman *software* dan ancaman pada data/informasi (Kemhan RI, 2014). Ancaman tersebut tentu saja berpotensi lebih besar saat *hardware* berada di luar kedaulatan kita sendiri.

Sumber daya pertahanan siber perlu dirumuskan mengingat banyak sekali peristiwa di dunia yang menggunakan media siber. Disamping kekuatan negara saat ini sudah tidak lagi dilihat hanya pada persenjataan yang dimiliki, melainkan pada budaya, ekonomi, politik dan peguasaan teknologi termasuk siber di dalamnya (Rahmawati, 2017). Berbagai kejadian serangan sistemik terhadap infrastruktur penting sebuah negara telah mengejutkan dunia, terlebih lagi pelakunya tidak hanya *state actor*, melainkan *non state actor* juga ikut berperan. Kejadian di belahan dunia lain adalah contoh nyata dan berharga bahwa peristiwa biasa dilatar belakangi dan menggunakan media siber dalam eksekusi pelaksanaannya.

Kerugian kejahatan siber tidak bisa disepelekan. Di Indonesia, kerugian kejahatan siber mencapai Rp. 194,6 miliar pada kurun waktu tahun 2015 hingga Februari 2016 (Symantec, 2016). Jumlah yang tidak sedikit mengingat peningkatan

transaksi elektronik dari tahun ke tahun semakin meningkat dan lebih meningkat lagi pada masa pandemi Covid-19 ini.

Sumber daya pertahanan siber terlihat biasa saja, namun sangat penting dalam menghadapi serangan dari berbagai pihak yang menggunakan media siber untuk menjalankan niat dan pemufakatan jahat terhadap kepentingan kita. Mengutip pernyataan

Bapak Persandian Republik Indonesia Mayjend TNI DR. Roebiono Kertopati, bahwa :

"(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menyebabkan Keruntuhan Negara"

Penyataan tersebut merupakan peringatan kepada kita semua untuk senantiasa waspada. Penyerang menunggu bagian yang paling lemah dalam keadaan tidak siaga dan potensi tersebut salah satunya pada bidang siber. Kondisi keamanan siber dapat membuat sebuah negara bisa dilumpuhkan dan dihancurkan menggunakan perang siber (Brantas, 2014). Untuk itu, sumber daya pengamanan siber harus dilaksanakan oleh seluruh entitas PSE yaitu pemilik data (*data owner*), pengelola data (*data custodian*), hingga pembuat kebijakan (*regulatoy body*). Sinergi dari entitas tersebut dilaksanakan untuk menentukan resiko dan kendali objektif dari data yang digunakan dalam sistem elektronik.

Pemilik data (*data owner)* merupakan pertahanan pertama dari sekumpulan data yang lebih besar. Pemilik data harus memastikan data pribadinya tidak sembarangan dibagi kepada pihak tertentu. Pengelola data (*data custodian*) memiliki andil yang besar dalam mengamankan data orang lain. Pengelola data boleh menjual data secara anonim kepada pihak lain. Misalnya adalah jumlah pengguna layanan "A" pada kota Jakarta. Hal tersebut dibenarkan dan tidak bertentangan dengan hukum yang ada. Pembuat kebijakan (*regulatoy body*) merupakan bentuk kehadiran negara (*state)* dalam menjalankan kehidupan berbangsa dan bernegara warganya. Pembuat kebijakan harus mampu menutup semua celah yang memunngkinkan serangan siber masuk dan menjalankan niatnya. Pembuat kebijakan sangat berpengaruh mengingat *cybersecurity*

merupakan sebuah ekosistem yang terdiri atas hukum (*laws),* kemampuan *(skill),* kerjasama *(cooperation)* dan implementasi teknis yang berjalan selaras dapat menjadikan keamanan siber menjadi optimal (ITU, 2017). Hukum yang menjadi payung dalam setiap kegiatan pertahanan siber ini dilaksanakan dengan harmonis dan sesuai standar meliputi legislasi (*legislation),* penindakan (*criminal enforcement)* dan *judicial review* dalam proses penegakan hukum dan peradilanya (Makari, 2014).

Badan Siber dan Sandi Negara (BSSN) dalam memimpin pengamanan siber menyusun langkah-langkah sesuai amanat PP 71 tahun 2019. Konsep yang ditawarkan oleh BSSN adalah Strategi Keamanan Siber Nasional (SKSN) sebagai langkah nyata kehadiran negara dalam upaya mewujudkan keamanan dan ketahanan nasional di ruang siber. Konsep SKSN menurut kepala BSSN juga mencakup pembangunan budaya keamanan siber. Fokus strategi SKSN meliputi penataan manajemen resiko pada keamanan siber, menyiapkan ketahanan dan kesiapsiagaan infrastruktur informasi vital nasional, pembentukan kapabilitas dan kapasitas, kerja sama legislasi dan regulasi internasional. Hal tersebut merupakan regulasi yang sedang disiapkan sebagai tindak lanjut revisi PP 71 tahun 2019. Sebagai satuan pelaksana keamanan siber, BSSN membentuk *Computer Security Incident Response Team* (CSIRT). CSIRT bertanggung jawab dalam menerima, menganalisis dan menanggapi aktivitas dan laporan insiden keamanan siber. BSSN juga menggalakkan literasi dan edukasi budaya keamanan siber untuk mewujudkan ekosistem ruang siber yang aman. Tim tersebut selanjutnya dapat berkolaborasi dan meneruskan potensi ancaman ke pasukan siber *(cyberarmy)* yang bisa dibentuk dalam strategi pembangunan Pusat Pertahanan Siber (*cyber defense)* yang terdiri atas TNI AD, TNI AL, TNI AU dan kalangan sipil tertentu (Rahmawati, 2017 hal. 61).

Dalam pengamanan *big data,* beberapa pendekatan perlu dilakukan misalnya penerapan teknologi enkripsi yang sesuai dengan data yang tersimpan (teknik kriptografi). Dalam konsepsi komputasi awan para peneliti sedang mengembangkan *Homomorphic Encryption,* yang dapat menjadi solusi terhadap penyimpanan atau

transaksi data yang berada di "awan" (termasuk secara geografis tidak dalam batas wilayah kedaulatan negara). Disisi strategi terdapat pola pengembangan keamanan berlapis (*layered approach),* atau yang biasa dikenal dengan *"defense in depth"*, strategi ini juga dapat diterapkan pada penempatan data- data yang dinilai (melalui mekanisme penilaian resiko) dapat ditempatkan diluar negeri. Terakhir secara teknis penguatan perangkat ("*hardening device*") dan visibilitas (*SIEM Technology*) terhadap keamanan data harus menjadi syarat utama penempatan data yang dilakukan diluar negeri.

TNI AU dalam melaksanakan operasi informasi memerlukan konsep yang adaptif terhadap perkembangan teknologi informasi termasuk regulasi yang menaunginya. Implementasi PP 71 tahun 2019 terhadap operasi informasi TNI AU diawali dengan pengamanan *data center* dan *data recovery center* baik yang berada di dalam negeri maupun di luar kedaulatan negara. Tindakan kontijensi ini harus dilaksanakan pertama kali saat kondisi negara, kondisi regional dan internasional tidak kondusif. *Profilling* warga negara Indonesia secara optimal yang berasal dari data yang dimiliki oleh pemerintah ditambah dengan pengolahan data dari aplikasi pihak ketiga. Dengan pengumpulan data secara lengkap akan memudahkan analisa cara bertindak musuh untuk menyerang. Langkah selanjutnya adalah melaksanakan *profilling* warga negara asing sesuai dengan proyeksi ancaman yang telah dirumuskan. *Profilling* tersebut ditujukan untuk menndapatkan data perorangan dengan menggunakan data layanan di dalam negeri.

Pengamanan *big data* menjadi tidak ideal saat infrastruktur *big data* berupa berada di luar wilayah kedaulatan sendiri dan tidak adanya undang undang perlindungan data di Indonesia yang melindungi data tersebut (Bisnis Tempo, 30 Desember 2020). Sebagian besar *stake holder* menyampaikan pandangan bahwa sebaiknya seluruh *data center* dan *data recovery center* baik lingkup privat dan publik berada di Indonesia. Meskipun memiliki konsep pengamanan *big data,* namun dari pandangan awal seluruh *stake holder* pada saat proses revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 merupakan kondisi ideal yang harus dilaksanakan, maka sebaiknya

data center dan *data recovery center* berada di wilayah NKRI. Selanjutnya Undang-undang PDP yang belum disahkan, sebaiknnya melihat isi UU dari 136 negara lain, sehingga prinsip privasi, transparansi, otonomi, non diskrimasi dapat tercapai (Yvonne, 2017). Kedua kondisi tersebut jika terlalu lama dibiarkan maka serangan siber akan sering terjadi, karena tidak adanya sanksi yang jelas dan membuat efek jera, maka sebaiknya penngaturan dilaksanakan dengan merevisi PP 71 tahun 2019 dengan menambahkan sanksi yang jelas dan merubah aturan penempatan *data center* menjadi di wilayah NKRI.

5. Kesimpulan

Kesimpulan yang dapat diambil pada tulisan ini adalah sebagai berikut :

a. Revisi pada PP 82 tahun 2012 menjadi PP 71 tahun 2019 pada infrastruktur *big data* berupa *data center* dan *data recovery center* dilatar belakangi oleh pengaturan yang masih bersifat umum pada PSE publik dan privat, perkembangan terknologi elektronik serta tuntutan pengamanan terhadap data. Dampak revisi PP 82 tahun 2012 menjadi PP 71 tahun 2019 adalah dampak ekonomi berupa potensi pajak yang hilang, berkurangnya potensi lapangan kerja, tambahan biaya koneksi internet dan kepastian investasi mennjadi terganggu. Dampak revisi selanjutnya adalah bidang pengamanan data yang lebih kompleks, bidang legislasi berupa turunan PP 71 tahun 2019 yang mendesak untuk dilaksanakan dan kedaulatan data yang sulit terpennuhi.

b. Sumber daya pengamanan siber yang dapat dipersiapkan adalah pemilik data, pengelola data dan pembuat kebijakan.

c. Konsep pengamanan *big data* adalah dengan menegakkan kewajiban syarat keamanan informasi, enkripsi, *layered approach* dan *hardening device.* Pelaksanaan operasi informasi tidak mengalami kendala jika data center berada di Indonesia karena pengamanan baik secara *hardware* maupun *software* dapat dilaksanakan dengan maksimal.

6. Ucapan Terima Kasih

Dalam penyusunan dan penulisan penelitian ini tidak terlepas dari bantuan bimbingan serta dukungan dari berbagai pihak. Oleh karena itu dalam kesempatan ini penulis dengan senang hati menyampaikan ucapan terima kasih yang sebesar-besarnya kepada yang terhormat Dosen Pembimbing, Nara Sumber, Kementerian Kominfo, BSSN, Unhan RI, Seskoau dan Seluruh sahabat dimanapun berada.

Daftar Pustaka

Alberts, S David (1996), Defensive Information Warfare, National Defennse University, Washington DC.

Anggoro, K. (2011). *Perang Asimetris: global, regional dan nasional*, in Seminar "Menjawab Tantangan Perkembangan *Asymetric Warfare* di Kawasan nasional, regional dan internasional", Indonesia Defense University. Jakarta

Ardiyanti, Handrini (2018), Swafoto: Sebuah Pendekatan Teori Manajemen Privasi Komunikasi", Fisip UI. Depok.

Aryasa, K. (2015). Big Data: Challenges and Opportunities. In Workshop Big Data Puslitbang Aptika dan IKP, tanggal 19 Mei 2015. Puslitbang Aptika dan IKP.

A.S, Aa Bambang, and Idealisa Fitriana. "Cyberterrorism: suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional." *Inter Komunika*, vol. 2, no. 1, 2017, pp. 1-15, doi:10.33376/ik.v2i1.12.

Bifet, Alber (2012), Mining Big Data In Real Time, Barcelona, Spain.

Cox, L. Joseph (2006), "Information Operation in Operations Enduring Freedom and Iraqi Freedom-What Went Wrong?". USA Command and Generall Staff College, Kansas

Denning, E. Dorothy (1998), Information Warfare and Security, ISBN :0201433036, Addison-Wesley.

Esterberg, K.G. (2002), "*Qualitative Methods in Social Research"* Bostonn, MA. McGrawHill.

Irwansyah dan Winarsih (2020), Proteksi Privasi Big Data dalam Media Sosial, Jurnal Audience :Jurnal Ilmu Komunikasi, Universitas Indonesia.

Jianqing Fan, Fang Han, Han Liu, Challenges of Big Data analysis, *National Science Review*, Volume 1, Issue 2, June 2014, Pages 293 314, https://doi.org/10.1093/nsr/nwt032

Jonni Mahroza, Priyanto Priyanto, Mhd Halkis, (2022) Asymmetric Diplomacy And Securitization In The South China Sea Vol 11,No,.1, http://ajis.fisip.unand.ac.id/index.php/ajis/article/view/567

Kuner, Christopher, Cate H.Fred, Milliard, Christopher, Stephenson Danker (2012) The Challenge of Big Data for Data Protection, Oxford University.

Miles, M.B., & Michael Huberman, A. (1994) *Qualitative Data Analysis (2nd ed)* Sage Publication

Moreno Julio, Serrano A. Manuel, and Fernandez-Medina Eduardo," Main Issues in Big Data Security", University of Castila-La Mancha, Spain.

Nugroho FP, Abdullah RW, Wulandari S, Hanafi (2019). Keamanan Big Data di Era Digital di Indonesia, STIE "AUB". Surakarta

Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure. USA: State University of New York

Putra, Ratno Dwi, Supartono, Supartono, & Deni, D. A. R. (2018). Ancaman Siber Dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). Peperangan Asimetrik, 4(2).

Rohendi, A. (2020). Perlindungan Hukum Big Data. *Jurnal Sain Manajemen*, 2(2), 1-5. Retrieved from http://ejurnal.ars.ac.id/index.php/jsm/article/view/300

Sofaer, S. (1999). "Qualitatife Methods: What Are They and Why Use Them?" Health Service Research. New York.

S. Madden, "From Databases to Big Data," in IEEE Internet Computing, vol. 16, no. 3, pp. 4-6, May-June 2012, doi: 10.1109/MIC.2012.50.

Suwardana, Hendra (2018). Revolusi Industri 4.0 Berbasis Revolusi Mental. Universitas Ronggolawe, Tuban.

Stacioiu, Alin (2017) The Fourth Revolution Industrial, Industry 4.0, Academia Brancusi, Targu Jiu.

T. A. Berson and D. E. Denning, "Cyberwarfare," in IEEE Security & Privacy, vol. 9, no. 5, pp. 13-15, Sept.-Oct. 2011, doi: 10.1109/MSP.2011.132.

Y. Demchenko, C. de Laat and P. Membrey, "Defining architecture components of the Big Data Ecosystem," 2014 International Conference on Collaboration Technologies and Systems (CTS), Minneapolis, MN, USA, 2014, pp. 104-112, doi: 10.1109/CTS.2014.6867550.

Zhang, Dongpo (2018), "Big Data Security and Privacy Protection," 8th International Conference on Management and Computer Science (ICMCS 2018), Henan, China.