Jurnal Lembaga Ketahanan Nasional Republik Indonesia

KONSTRUKSI PERTAHANAN DAN KEAMANAN NEGARA TERHADAP PERLINDUNGAN DATA DALAM *CYBERSPACE* UNTUK MENGHADAPI POLA KEBIASAAN BARU

The Construction of State Defense and Security Against Data Protection in Cyberspace to Facing New Habits

Muhammad Irfan Hilmy[1], Rama Halim Nur Azmi[2],
[1]Fakultas Hukum, Universitas Brawijaya, irfanhilmy37@gmail.com,082298124673
[2]Fakultas Hukum, Universitas Brawijaya, halimrama16@gmail.com,082178193928

ABSTRAK: Pandemi COVID-19 saat ini telah meningkatkan interaksi di dunia maya (*cyberspace*) terutama dalam arus data dikarenakan adanya pola kebiasaan baru yakni pekerjaan dan pembelajaran dilaksanakan secara daring. Tingginya intensitas interaksi di *cybperspace* berkorelasi lurus dengan tingginya angka serangan siber. Menurut data dari BSSN dalam rentang Januari hingga April 2020, serangan siber di Indonesia mencapai angka 80 juta. Tanpa adanya perlindungan yang jelas maka serangan tersebut dapat mengancam keamanan dan pertahanan negara. Penelitian ini bertujuan untuk menganalisis problematika pertahanan dan keamanan *cyberspace* Indonesia dan mengkonstruksikan konsep pertahanan dan keamanan negara dalam *cyberspace*. Metode yang digunakan dalam tulisan ini adalah yuridis normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konsep. Kesimpulan dari tulisan ini adalah dengan adanya peningkatan aktivitas dalam dunia mayantara yang berkenaan dengan perlindungan data sehingga perlindungan khusus terkait data dan tentunya mengancam kedaulatan negara oleh karenanya dalam rangka mengupayakan usaha pertahanan dan keamanan negara di *cyberspace* selain diperlukan undang-undang yang secara khusus mengatur terkait hal tersebut juga diperlukan adanya perjanjian timbal balik antara Indonesia dengan Negara lain untuk mengatasi serangan-serangan siber yang pelakunya berada di negara lain. Instrumen tersebut diperlukan untuk menciptakan langkah persuasif dan diplomatis untuk memperkuat hubungan kedua negara sehingga membuka ruang kedamaian bagi kawasan maupun global.

Kata kunci: COVID-19, *Cyberspace*, Pertahanan dan Keamanan Negara, Serangan Siber.

ABSTRACT: *The current COVID-19 pandemic has increased interactions in cyberspace, especially in the flow of data due to new habit patterns, namely work and learning carried out online. The high intensity of interactions in cyberspace correlates directly with the high number of cyberattacks. According to data from BSSN from January to April 2020, cyberattacks in Indonesia reached 80 million. Without clear protection, these attacks can threaten national security and defense. This study aims to analyze the problems of defense and security in cyberspace Indonesian and construct the concept of state defense and security in cyberspace. The method used in this paper is a normative juridical approach to legislation and a conceptual approach. The conclusion of this paper is that there is an increase in activity in the world with regard to data protection so that special protection is related to data and of course threatens the sovereignty of the state, therefore in order to strive for national defense and security efforts in cyberspace apart from required laws specifically regulating this matter. It is also necessary to have a reciprocal agreement between Indonesia and other countries to deal with cyber attacks where the perpetrators are in another country. These instruments are needed to create persuasive and diplomatic steps to strengthen relations between the two countries so as to open space for peace for the region and globally.*

Keywords: *COVID-.19, Cyberspace, State Defense and Security, Cyberattacks.*

PENDAHULUAN

Pertahanan dan keamanan negara merupakan salah satu hal mendasar dalam rangka menjaga dan mempertahankan kedaulatan negara. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) sebagai *staatsfundamentalnorm* yang melandasi penyelenggaraan kehidupan berbangsa dan bernegara pada bagian Aline Keempat Pembukaan telah menyatakan secara tegas bahwa yang menjadi tujuan negara yakni melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Rumusan *in abstracto* pada bagian Pembukaan tersebut kemudian dituangkan pada Bab XII tentang Pertahanan dan Keamanan Negara. Dikarenakan keberadaan UUD NRI 1945 dalam hierarki peraturan perundang-undangan berada pada posisi pertama maka rumusan- rumusan dalam UUD NRI 1945 tersebut perlu dituangkan secara rinci dalam produk undang- undang organik. Adapun undang-undang terkait pertahanan negara yakni Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Dalam paradigma konvensional usaha pertahanan dan keamanan negara diartikan sebagai upaya untuk melindungi dan mempertahankan negara baik di darat, laut maupun udara. Namun, saat ini paradigma tersebut telah berubah seiring dengan perkembangan teknologi informasi dan telekomunikasi. Salah satu hal yang eksis di era serba teknologi saat ini adalah hadirnya wilayah non fisik yakni ruang maya atau biasa disebut *cyberspace*. Abdul Wahid dan Muhammad Labib mendefinisikan *cyberspace* sebagai suatu realitas baru yang tercipta karena adanya teknologi internet di mana interaksi antarmasyarakatnya terjadi secara *virtual* dan melalui lintas batas negara (Wahid, 2005) .

Adanya realitas baru yakni dunia maya telah menyebabkan bergesernya konsep perang antarnegara yang sebelumnya terbatas pada peperangan secara fisik tetapi juga perang dalam dunia maya atau lebih dikenal dengan istilah *cyber war* (Rahmawati, 2017). Dalam konsepsi *cyber war* pelaku atau aktor dalam perang tersebut tidak hanya terbatas pada negara saja tetapi juga individu atau kelompok *hacker*, organisasi non pemerintahan (*non-governmental organization*), jaringan teroris, kelompok kejahatan terorganisasi, maupun sektor swasta seperti *internetand provider company* (Pearlman, 2012).

Adapun motif yang melatarbelakangi terjadinya *cyber war* tersebut dapat berupa kepentingan ekonomi, politik, militer, ideologi, maupun budaya. Tanpa adanya mekanisme pertahanan dan kemanan dalam dunia maya tersebut dapat menciptakan celah bagi negara maupun aktor lainnya untuk mengintervensi kedaulatan negara. Intervensi tersebut dilakukan dengan melakukan pencurian informasi, penyebaran berita *hoax,* propaganda, indoktrinasi, atau penyerangan terhadap sistem informasi vital seperti *website* pemerintah, jaringan militer, atau sistem pertahanan negara (Smith, 2015).

Sejak awal tahun 2020, Indonesia turut serta menjadi negara terinfeksi *Corona Virus Disease* 2019 (COVID-19). Di tengah situasi pandemi COVID-19 masyarakat harus menerapkan pola kebiasaan baru dalam segala lini kehidupan. Dalam sektor kerja dan pendidikan diterapkan mekanisme *work from home* dan *study from home*. Pola kebiasaan baru tersebut mayoritas menggunakan media internet. Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) jumlah pengguna internet Indonesia meningkat menjadi 196,7 juta jiwa hingga kuartal II 2020. Adapun persentase jumlah pengguna internet tersebut sebesar 73,7% dari total penduduk Indonesia sejumlah 266 juta jiwa (Tim Asosiasi Penyelenggara Jasa Internet Indonesia, 2020).

Meningkatnya jumlah pengguna internet di Indonesia tersebut secara linear juga meningkatkan serangan siber di Indonesia. Data dari Badan Siber dan Sandi Negara (BSSN) yang mana dalam rentang waktu Januari hingga Agustus 2020 terdapat sekitar 190 juta upaya serangan siber di Indonesia. Angka tersebut meningkat 4 (empat) kali lipat apabila dikomparasikan dengan data tahun sebelumnya sebesar 39 juta. Mengutip pernyataan Sigit Kurniawan selaku Kasubdit Identifikasi Kerentanan dan Penilaian Risiko Infrastruktur Informasi Kritikal Nasional III BSSN dalam wawancaranya bersama Kompas dijelaskan bahwa peningkatan serangan siber tersebut terjadi karena adanya penerapan pola hidup baru masyarakat saat pandemi COVID-19 (Biro Hukum dan Kerjasama Badan Siber dan Sandi Negara, 2020).

Data tersebut merupakan suatu bukti konkret bahwa hingga saat ini dunia maya (*cyberspace*) Indonesia berada dalam kondisi rawan dari serangan siber. Hal tersebut tentunya membahayakan bagi sistem pertahanan dan keamanan negara. Apabila tidak adanya suatu konsep perlindungan yang jelas maka serangan siber di Indonesia akan terus meningkat. Akibat dari hal tersebut adalah tereduksinya kedaulatan negara bahkan dapat merugikan baik bagi kepentingan nasional maupun kepentingan warga negara.

Tulisan ini akan membahas mengenai bagaimana kondisi dunia maya (*cyberspace*) Indonesia selama ini dan kemudian bertitik tolak dari realita tersebut maka bagaimana urgensi perlindungan data dalam dunia maya (*cyberspace*) tersebut berkenaan dengan pertahanan dan keamanan negara. Tentunya penelitian ini tidak hanya berangkat dari segi teoritis saja tetapi juga dikaitkan dengan data-data yang ada secara nyata. Selain itu, penulis juga menganalisis terkait ketentuan peraturan perundang-undangan sehubungan dengan perlindungan data dalam dunia maya (*cyberspace*) di Indonesia.

METODE

Jenis penelitian dalam artikel ini adalah *yuridis normatif* atau disebut juga penelitian hukum doktrinal (B. S., (n.d)), yaitu peneliti menelaah bahan hukum primer (Hanitijo, 1988) kemudian dilanjutkan dengan penelitian terhadap bahan hukum sekunder untuk menjawab permasalahan yang menjadi fokus penelitian yang mengkonsepkan hukum sebagai kaidah atau norma yang merupakan patokan berperilaku manusia yang dianggap pantas. Metode pendekatan penulisan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan *(statute approach),* yaitu dengan menelaah dan menganalisis peraturan perundang-undangan yang berkaitan dengan pertahanan negara di ruang siber (Widnjoesoebroto, 2002). Pendekatan konsep (*conseptual approach*), yaitu menelaah konsep pertahanan negara dalam ruang siber (Marzuki, (n.d.)).

HASIL DAN PEMBAHASAN

Problematika Dunia Maya (*Cyberspace*) Indonesia

Merujuk pada ada yang dipublikasi oleh Statista jumlah pengguna Indonesia berada pada angka 143,26 juta per Maret 2019. Dengan jumlah pengguna internet sebanyak itu Indonesia menempati peringkat lima terpaut 5,8 juta dengan Brasil dengan jumlah pengguna internet sebanyak 149,06 juta (M. M. Lubis F. M., 2020). Pada tahun ini dikarenakan adanya pandemi COVID-19 yang mengakibatkan dibatasinya interaksi secara fisik maka terjadi peningkatan terhadap jumlah pengguna internet di Indonesia. Sehingga sebagaimana dikemumakan oleh Direktur Jenderal Penyelenggaraan Pos dan Informatika Kementerian Komunikasi dan Informasi, Ahmad M. Ramli bahwa di tengah situasi pandemi seperti saat ini internet dianalogikan sebagai oksigen karena hampir seluruh kegiatan mulai dari sekolah, bekerja, hingga belanja

dilakukan secara daring karena tidak memungkinkannya dilakukan secara luring akibat pandemi (Hakam, 2020).

Meskipun secara statistik Indonesia memliki jumlah pengguna internet terbesar kelima di dunia pada 2018 tetapi hal tersebut tidak berkorelasi positif dengan aspek ketahanan dan keamanan siber di Indonesia. Apabila ditelisik sesungguhnya Indonesia merupakan negara yang rentan terhadap ancaman perang siber. Pada tahun 1998, Indonesia terlibat perang siber dengan Tiongkok dan Taiwan berkaitan dengan konflik sosial dan politik. Kemudian di tahun berikutnya Indonesia kembali terlibat perang siber dengan Portugal berkenaan dengan kasus referendum Timor Timur (Manthovani, 2006).

Bahkan Presiden Republik Indonesia keenam yakni Susilo Bambang Yudhoyono pernah menjadi target penyadapan pada tahun 2013. Tindakan penyadapan tersebut dilakukan oleh badan intelijen Australia bersama *National Security Agency* (NSA) Amerika Serikat. Target penyadapan tersebut tidak hanya kepada Presiden Susilo Bambang Yudhoyono tetapi juga kepada istri, dan orang-orang yang berada di lingkungannya (Tanter, 2014). Seorang Presiden selain sebagai kepala pemerintahan juga merupakan seorang kepala negara yang menjadi simbol martabat suatu negara. Kasus Presiden Susilo Bambang Yudhoyono tersebut merupakan suatu pukulan telak bagi Indonesia di mana ketiadaan mekanisme perlindungan terkait pertahanan dan keamanan negara dalam dunia maya (*cyberspace*). Sehingga secara eksplisit hal tersebut menunjukkan bahwa Indonesia merupakan negara yang rawan akan serangan-serangan siber tersebut.

Menurut data dari BSSN, dalam rentang Januari-Maret 2020, total serangan siber di Indonesia mencapai 80.837.445. Angka tersebut naik 6 (enam) kali lipat dibandingkan serangan pada periode Januari-Maret 2019 yang berjumlah 13. 623.527 (Miarsa, 2020). Sebanyak 56% dari total serangan dalam rentang Januari-Maret 2020 merupakan *trojan activity*, 43% merupakan *information gathering*, dan 1% *web application attack* (Hadi, 2020).

Berdasarkan pemantauan yang dilakukan oleh BSSN, situs pemerintah juga merupakan salah satu target serangan siber di Indonesia. Tercatat dalam kurun waktu 1 Januari-12 April 2020 sebanyak 159 kasus *web defacement* terjadi di Indonesia. Adapun rincian dari kasus tersebut yakni 16 kasus di bulan Januari, 26 kasus di bulan Februari, 69 kasus di bulan Maret, dan 48 kasus sampai dengan perkembangan terakhir yakni 12 April 2020. Berkaca dari hal tersebut dapat dilihat bahwa ancaman terhadap serangan siber di Indonesia tidak dapat dipandang sebelah mata. Hal tersebut dikarenakan serangan-serangan tersebut secara perlahan dapat mengancam keutuhan negara.

Apabila merujuk pada data yang dirilis oleh *Central Intelligence Agency* (CIA) kerugian akibat serangan dan kejahatan siber di Indonesia mencapai angka USD 895 billion atau sekitar 1,20% dari total keseluruhan perkiraan kerugian secara global yang mencapai USD 71,620 *billion*. Kerugian yang muncul akibat serangan dan kejahatan siber tersebut haruslah menjadi konsentrasi semua pihak. Perlu menjadi kesadaran bersama bahwa hingga saat ini tidak adanya mekanisme yang jelas mengenai sistem pertahanan dan keamanan negara dalam dunia maya (*cyberspace*) di Indonesia.

Secara yuridis, Indonesia sampai saat ini belum memiliki produk peraturan perundang-undangan yang mengatur terkait pertahanan dan keamanan negara dalam dunia maya. Apabila dikomparasikan dengan Tiongkok dapat diketahui bahwa angkatan bersenjata Tiongkok tidak hanya sebatas matra darat, laut, atau udara tetapi juga ditambahkan ruang angkasa dan ruang siber. Sedangkan di Indonesia paradigma konsepsi pertahanan dan keamanan siber belum terlihat titik

terang bagaimana kebijakan yang harus dilaksanakan. Padahal apabila dilihat rekam jejak Indonesia sejak dahulu hingga saat ini bahwa negara ini rentan terhadap serangan-serangan siber. Guna menghadapi pola kebiasaan baru ke depannya dan melihat bahwa penetrasi internet di Indonesia yang sangat tinggi maka perlu adanya suatu sistem pertahanan dan keamanan siber di Indonesia.

Urgensi Perlindungan Data Dalam Perspektif Pertahanan Negara

Berkembangnya dunia tanpa batasan ruang seperti saat ini, memberikan kesempatan pada setiap orang untuk mengakses apapun dalam waktu singkat untuk melihat apa yang sedang terjadi dalam ruang lainnya. Simulasi sederhananya adalah orang Indonesia tidak perlu pergi ke Amerika Serikat untuk melihat kejadian kebakaran gedung disana, melainkan hanya dengan mengakses platform digital menggunakan jaringan internet maka hal-hal yang berkaitan dengan kebakaran gedung di Amerika Serikat dapat dilihat dari Indonesia. Simulasi sederhana tersebut menunjukkan akses yang tidak terbatas dalam hal mendapatkan informasi dari bagian dunia lainnya tanpa perlu mendatanginya langsung. Dalam konteks ini mungkin kemampuan dan kesempatan tersebut merupakan hal yang positif dan dapat diterima sebagai suatu berkah bagi kemajuan pengetahuan manusia. Namun disisi lain, berbagai hal negatif membayangi keadaan tersebut dan bahkan bisa menjadi petaka bagi keamanan dan ketahanan sebuah negara dalam mengelola wilayahnya (dalam rangka kedaulatan negara).

Pergeseran ancaman bangsa dan negara menjadi tema utama dalam penguatan skema pertahanan dan keamanan untuk menciptakan situasi kondusif bagi kehidupan berbangsa dan bernegara. Ancaman fisik bukanlah menjadi satu-satunya hal yang perlu diwaspadai dan dicegah dampaknya, tetapi adanya ancaman dalam dunia mayantara menjadi entitas baru dalam kehidupan modern saat ini. Ancaman ini yang kemudian dikenal dengan ancaman siber yang berkaitan dengan ruang mayantara. Berbeda dengan ancaman fisik yang dapat dideteksi secara visual, ancaman siber lebih sukar untuk dideteksi karena memerlukan keahlian khusus untuk mendeteksinya.

Ancaman siber ini dapat menjadi ancaman nyata bagi kedaulatan negara, mengingat ancaman ini dapat menyerang sistem siber yang berisikan data-data penting yang dimiliki oleh Indonesia. Misalnya peretasan *big data* yang berkaitan dengan kependudukan masyarakat. Di Amerika serikat sendiri beberapa bulan terakhir banyak menghadapi ancaman siber yang berkaitan dengan peretasan terhadap data penduduk, misalnya pada Bulan Oktober yang lalu *The U.S Department of Homeland Security* (Departemen Keamanan Dalam Negeri Amerika Serikat) berhasil mendeteksi adanya upaya peretasan terhadap biro sensus Amerika Serikat untuk mengumpulkan data milik masyarakat dan merubah informasi pendaftaran (Center for Strategic & International Studies, 2020). Upaya tersebut tentu berbahaya bagi pertahanan Amerika Serikat karena memungkinkan pemetaan terhadap kelemahan negara, misalnya dari upaya peretasan tersebut ada upaya untuk memetakan rata-rata usia penduduk suatu daerah sehingga peretas mengetahui daerah-daerah yang memiliki masyarakat dengan mayoritas usia lansia atau muda. Tidak hanya itu, peretasan terhadap biro sensus tersebut memungkinkan pula untuk menghambat terselenggaranya pesta demokrasi negara sehingga mengakibatkan instabilitas keadaan disana. Amerika Serikat memang menjadi negara yang mendapatkan serangan luar biasa dari serangan dalam dunia siber. Menurut FBI saja selama 2020 ini ada sekitar 4.000 serangan siber yang dilaporkan kepada divisi siber dibawah naungan FBI. Berdasarkan statistik, masifnya

serangan tersebut meningkat selama pandemi COVID 19 yang terjadi sepanjang 2020.

Kasus *cyber security* yang berkaitan dengan data juga terjadi di negara Singapura pada akhir 2019 lalu. Kasus tersebut berkaitan dengan kebocoran data milik personel *Ministry of Defence* dan *Singapore Armed Forces* yang terjadi akibat aktivitas *phishing email* dengan *malware* berbahaya yang dikirimkan ke akun-akun milik 2400 personel (Allianz Global Corporate & Speciality, 2020). Pada kasus lain data 120.000 orang termasuk di dalamya 98.000 personel *Singapore Armed Forces* dideteksi telah terinfeksi *ransomware* pada awal Desember 2019. Pada dua kasus tersebut menunjukkan bahwa semua orang dapat menjadi korban pencurian data bahkan aparatur militer ataupun orang-orang yang berada pada sektor pertahanan dan keamanan negara.

Indonesia sendiri pernah mengalami beberapa beberapa serangan siber yang berkenaan dengan data. Salah satunya adalah konflik di ruang siber antara Indonesia dan Portugal dalam kasus Timor Timur pada tahun 1999 yang dikabarkan hingga masuk ke dalam sistem dan bahkan dapat menghapus semua data yang ada di dalam sistem.

Tentu keadaan ini mengancam bagi keberlangsungan negara. Dengan mudah negara lain dapat mengetahui berbagai macam data yang mengarah pada identifikasi terhadap kelemahan kekuatan pertahanan yang dimiliki oleh Indonesia. Oleh karenanya mekanisme penguatan *cyber security* dalam hal ini adalah perlindungan data perlu diprioritaskan untuk dapat melindungi serta meminimalisir segala ancaman terhadap kerahasiaan, integritas dan juga ketersediaan informasi (Ardiyanti, 2014) suatu negara.

Perlunya perlindungan terhadap data yang biasa tersimpan dalam *big data* akan mencegah terjadinya hal-hal yang mengganggu stabilitas keamanan suatu negara. Mengingat *big data* menjadi aset yang strategis bagi dunia industri, bisnis, kesehatan serta untuk melakukan eksplorasi terhadap dunia ekonomi (Sun, 2012). Dengan begitu peretasan pada *big data* dapat mengakibatkan kekacauan yang strategis terhadap berbagai bidang bahkan pertahanan. Menurut Petersson dan Breul, *big data* memiliki peluang untuk melihat ke dalam berbagai aspek data yang sebelumnya belum pernah dikumpulkan bahkan yang tidak pernah dianggap sebagai data. Sehingga dengan menganalisa *big data,* pembaca *big data* dapat melihat dan memetakan kekuatan serta kelemahan dari negara-negara lain (Petersson, 2017).

Dalam ranah ekonomi memang data yang ada di dalam *big data* sangat berdampak positif bagi laju industri karena dengan begitu perusahaan dapat dengan mudah untuk memetakan konsumen produknya bahkan dianggap sebagai "tambang emas" dunia di abad ke 21 (Solove, 2013). Bahkan untuk melindungi penyalahgunaan terhadap "tambang emas" tersebut, Uni Eropa membentuk satu payung hukum yang melindungi masyarakatnya dibawah hukum yang bernama GDPR (*General Data Protection Act*). Dengan sifatnya yang ekstra-teritorial, GDPR dapat menjangkau ke dalam perusahaan Uni Eropa yang berada di luar Eropa untuk tunduk pada ketentuan ini, demi melindungi hak privasi masyarakat Uni Eropa di seluruh dunia. Hal tersebut tentu berbanding terbalik apabila melihat dalam sektor pertahanan dan keamanan negara. Kebocoran data melalui *big data* tentu sangat berbahaya bagi sistem pertahanan karena memungkinkan peretas untuk menyalahgunakan data tersebut untuk kepentingan yang merugikan ketahanan nasional. Di sisi lain sebenarnya ada keharusan serta kewajiban dalam privasi pada *big data* untuk dilindungi yakni dalam perihal identitas, keamanan, kesetaraan, dan kepercayaan (Richards, 2016). Namun tentu tidak mudah melindungi hal tersebut mengingat ruang siber menjadi ruang yang tidak mudah untuk dijamah sehingga perlu kemampuan khusus untuk melihat indikasi kebocoran data ini.

Kebocoran data dalam perspektif pertahanan negara setidaknya menghasilkan beberapa dampak seperti pemetaan pada sarana strategis terkait dengan kekuatan penduduk serta terhadap kelemahan pertahanan negara yang ditinjau dari aspek kekuatan pasukan. Bahkan kebocoran data ini dapat mengakibatkan tersadapnya informasi-informasi strategis penting berkaitan dengan pertahanan negara. Membangun Konstruksi Hukum Perlindungan Data Dalam Pertahanan Negara

Sejak tahun 2012 lalu DPR telah melakukan pembahasan mengenai RUU Perlindungan Data Pribadi untuk menjawab tantangan zaman, mengingat UU 11 tahun 2008 tentang Informasi dan Transaksi Elektronik belum mengakomodasi secara spesifik mengenai ketentuan dalam perlindungan data pribadi.

Namun dalam kerangka pertahanan negara, selain membentuk perlindungan hukum terhadap data secara internal, pemerintah dengan DPR perlu mengambil ancang-ancang untuk mengadakan perjanjian timbal balik (*mutual legal assistance)* dengan negara lain mengingat kejahatan ini merupakan kejahatan *borderless* (tidak mengenal batasan wilayah) sehingga sangat dimungkinkan adanya peretasan ataupun pencurian data yang dilakukan pada yurisdiksi negara lain.

Dalam hukum internasional, Konvensi yang diadakan pada tahun 2001 di Budapest telah berusaha untuk menyatukan pandangan terhadap penegakan hukum siber yang salah satunya menyinggung persoalan data. Konvensi yang digagas oleh Uni Eropa tersebut kemudian dikenal dengan *Convention on Cyber Crime* yang salah satu tujuannya adalah memperkuat kerjasama internasional dalam mengurangi penyimpangan dalam menggunakan sistem, jaringan maupun data agar masyarakat terlindungi dari segala kejahatan siber (Syahdeini, 2009). Namun Konvensi ini memang memiliki fokus utama terhadap perkembangan dunia komputer sehingga aturan yang terdapat dalam Konvensi ini mengatur khusus mengenai perlindungan dalam komputer. Meskipun begitu Konvensi ini dapat menjadi tonggak hukum terhadap perlindungan data karena diantaranya meregulasi terhadap pengaturan keamanan data di dalam komputer.

Pengaturan tersebut diantaranya berkaitan dengan perintah terhadap negara yang tunduk pada Konvensi ini untuk mengatur pengaksesan secara tidak berhak (Pasal 2), Intersepsi secara tidak berhak (Pasal 3), Interferensi data (Pasal 4), dan lain sebagainya. Pada utamanya, Konvensi ini berusaha melindungi segala tindakan tanpa hak dengan hal yang berkaitan pada komputer.

Dalam rangka penegakan perlindungan data untuk mensolidkan ketahanan dan keamanan negara maka Indonesia perlu mengadakan *mutual legal assistance* dengan negara lain. Sebenarnya dalam kerangka hukum nasional, Indonesia telah memiliki UU yang mengatur mengenai *mutual legal assistance* yakni UU Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik. Namun dalam pelaksanaannya UU ini belum dapat memberikan dampak yang signifikan terhadap penanganan kejahatan siber. Permasalahan seperti ego sektoral masing-masing institusi penegak MLA menjadi salah satu alasannya.

Tumbuhnya kesadaran untuk membentuk kerjasama berkaitan dengan *mutual legal assistance* telah dipraktikkan awalnya oleh Amerika Serikat dan Swiss yang dilakukan pada 1972, kemudian ditandatangani pada 1973, dan baru efektif pada 1977. Untuk menindak lanjuti perjanjian tersebut maka pada tahun 1987 ditandatangani *memorandum of understanding* (MoU) antara kedua negara yang bertujuan untuk melengkapi ketentuan pada 1973. MoU ini kemudian dikenal dengan *MoU on Mutual Assistance in Criminal Matters and Anciliary Administrative Proceedings* (Sasmita, 2000).

Lahirnya kesadaran tersebut berawal dari

permasalahan yang tidak dapat ditegakkan oleh hanya satu yurisdiksi negara melainkan perlu peran negara lain untuk saling bekerja sama dalam mengenai kejahatan. Maka untuk kejahatan transnasional selain dengan adanya Konvensi, dibutuhkan pula aturan hukum lainnya seperti *mutual legal assistance* dalam mempertegas dan mempermudah penegakan hukumnya. Bahkan kerja sama ini harus dibentuk tidak hanya pada satu kawasan melainkan secara global untuk mensolidkan negara-negara di dunia dalam menghadapi kejahatan siber mengenai data.

Dalam perspektif pertahanan negara, perlindungan terhadap data dapat diasosiasikan pada pembatasan tindakan intelijen negara lain dalam mengawasi maupun memata-matai warga negara lain melalui data. Dalam konteks kedaulatan hal tersebut tentu berpotensi mengganggu stabilitas keamanan karena apabila data tersebut dipersalahgunakan oleh negara yang sedang memata-matai maka dapat berbahaya bagi kesatuan maupun keutuhan negara.

Oleh karenanya mengkonstruksikan hukum terhadap perlindungan data dalam ranah internasional melalui *mutual legal assistance* menjadi cara yang tepat untuk mempermudah penegakan hukum. Selain itu hal ini juga untuk mengatur dalam hal membatasi operasi intelijen negara lain berkaitan dengan *surveillances* pada data milik Indonesia. Pembatasan terhadap operasi intelijen ini tentu sangat penting mengingat dalam sejarahnya operasi intelijen yang berkaitan dengan pengumpulan data telah menyebabkan Kekaisaran Jepang menang dalam Perang Pasifik (Ken, 2009).

Untuk menghindari tindakan-tindakan *surveillance* terhadap Indonesia dalam perlindungan data sekaligus untuk mencegah pemetaan terhadap kelemahan negara melalui operasi pengumpulan data dan informasi oleh negara lain secara melawan hak maka perlu diadakan *mutual legal assistance* dengan negara lain. Dengan penggunaan perjanjian ini pula maka dapat terbangun keharmonisan antar negara mengingat *mutual legal assistance* merupakan kerjasama yang sangat persuasif dan diplomatis sehingga dapat memperkuat hubungan antar negara yang mengadakan perjanjian.

Sebagai bahan perbandingan, sekiranya tinjauan terhadap tindak pidana korupsi yang telah dianggap sebagai musuh bersama umat manusia (*hostis humanis generis)* dalam hal ini telah diadakan *mutual legal assistance* bersama beberapa negara yang menjadi langkah jitu dalam menangani korupsi yang salah satunya adalah untuk mencegah larinya terdakwa ke negara lain. Korupsi yang berdampak sangat besar bagi proses birokrasi dan keadaan ekonomi negara memang perlu perhatian besar sehingga wajar apabila negara memberikan perhatian khusus terhadap korupsi. Sehingga dalam hal pertahanan, negara harus pula memberikan perhatian khusus sebagai langkah pencegahan terhadap tindakan yang melemahkan pertahanan negara melalui kejahatan siber dalam data. Oleh karenanya pembentukan *mutual legal assistance* terkait dengan perlindungan data juga diperlukan sebagai langkah preventif untuk memperkuat pertahanan negara.

SIMPULAN

Dengan perkembangan zaman yang pesat dan keadaan global di tengah pandemi COVID 19 telah menyebabkan pergeseran ancaman terhadap keutuhan bangsa dan negara. Peningkatan terhadap penggunaan ruang mayantara melahirkan ancaman baru terkait kejahatan siber dalam bidang data yang dapat mengganggu ketahanan negara. Ancaman tersebut secara spesifik berupa kebocoran

data yang dapat mengakibatkan pemetaan terhadap kelemahan pertahanan Indonesia ataupun peretasan data yang mengakibatkan terganggunya sistem di Indonesia sehingga berpotensi menyebabkan instabilitas dalam masyarakat (misalnya meretas data kependudukan).

Dalam hal perlindungan data dalam pertahanan negara maka Indonesia perlu membuat suatu *mutual legal assistance* untuk melakukan pencegahan maupun penanganan dalam kejahatan ini. Instrumen ini tentu sangat relevan mengingat ancaman terhadap kejahatan data tidak hanya terjadi di Indonesia melainkan di berbagai negara. *Mutual legal assistance* sekaligus menjadi langkah persuasif dan diplomatis untuk memperkuat hubungan kedua negara sehingga membuka ruang kedamaian bagi kawasan maupun global.

DAFTAR PUSTAKA

Allianz Global Corporate & Speciality. 2020. *Allianz Risk Barometer Identifying The Major Business Risks For 2020*. München: Allianz.

Ardiyanti, H. 2014. Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica*, *5(1):* 95-110

B., S. n.d.. *Karakter Penelitian Hukum Normatif dan Sosiologis*. Yogyakarta: Puskumbangsi LEPPA UGM.Biro Hukum dan Kerjasama Badan SIber dan Sandi Nasional. 2020. *Rekapitulasi Insiden Web Defacement Januari 2020-April 2020*. Jakarta: Badan Siber dan Sandi Nasional.

Center for Strategic & International Studies. 2020. *Significant Cyber Incidents Since 2006*. Washington D. C.: Center for Strategic & International Studies.

Hadi, M. D. S., Widodo, P., Putro, R. W. 2020. Analisis Dampak Pandemi Covid 19 di Indonesia Ditinjau dari Sudut Pandang Keamanan Siber. *Jurnal Kebangsaan, 1*(1).

Hakam, M. T., Levani, Y., Utama, M. R. 2020. Potensi Adiksi Penggunaan Internet pada Remaja Indonesia di Periode Awal Pandemi Covid 19. *Hang Tuah Medical Journal*, *17*(2).

Hanitijo, S. R. 1988. *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta: Ghalia Indonesia.

Ken, K. 2009. Japanese Intelligence in WWII: Successes and Failures. *NIDS Journal of Defense and Security*, *11*(2), 3–27.

M., M., Lubis, F. M. 2020. Analisis Penggunaan Media Sosial dan Penyebaran *Hoax* di Kota Medan. *Jurnal SImbolika, 6*(1)

Manthovani, R. 2006. *Problematika dan Solusi Penanganan Kejahatan Siber di Indonesia*. Jakarta: Malibu.

Marzuki, P. M. n.d. *Penelitian Hukum*. Jakarta: Kencana.

Miarsa, F. R. D., Romadhon, A. H. 2020. Pelanggaran Hukum dalam Tindakan Vandalisme di Ruang *Cyberspace*. *KAMBOTI Jurnal Ilmu Sosial dan Humaniora, 1*(1).

Pearlman, W., Cunningham, K. 2012. Non-State Actors, Fragmentation, and Conflict Processes. *Journal of Conflict Resolution*.

Petersson, G. J., Breul, J. D. 2017. *Cyber Society, Big Data and Evaluation*. New Jersey: Transaction Publishers.

Rahmawati, I. 2017. Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defence. *Jurnal Pertahanan & Bela Negara*, *52*.

Richards, N. M., King, J. 2016. Big Data and The Future For Privacy. In *Handbook of Research on Digital Transformation* (pp. 1–26).

Sasmita, R. A. 2000. *Pengantar Hukum Pidana Internasional*. Bandung: Refika Aditama.

Smith, M. 2015. *Research Handbook on International Law and Cyberspace*. Massachusetts: Edwar Elgar Publishing Limited.

Solove, D. J. 2013. Introduction: Privacy Self-Management and The Consent Dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Sun, Z., Strang, D. S., Pambel, F. 2018. Privacy and Security in The Big Data Pradigm. *Journal of Computer Information Systems*, *60*(2), 146–155.

Syahdeini, S. R. 2009. *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Grafiti.

Tanter, R. 2014. Indonesia, Australia and Edward Snowden: Ambiguous and Shifting Asymmetries of Power. *The Asia Pasific Journal*.

Tim Asosiasi Penyelenggara Jasa Internet Indonesia. 2020. Survei Pengguna Internet

APJII 2019-Q2 2020: Ada Kenaikan 25,5 Juta Pengguna Internet Baru di RI. *Buletin APJII, Edisi 74*.

Wahid, A., Labib M. 2005. *Kejahatan Mayantara (Cyber Crime)*. Jakarta: Refika Aditama.

Widnjoesoebroto, S. 2002. *Hukum, Paradigma, Metode, dan Dinamika Masalahnya*. Jakarta: ELSAM-HUMA.