Volume 15. Number 2. December 2020 Page 154-166

Pandecta

http://journal.unnes.ac.id/nju/index.php/pandecta

Analisis Hukum Kedaulatan Digital Indonesia

Siti Yuniarti[1] dan Erni Herawati[2]

[1,2]Business Law Program, Law Department, Faculty of Humanities, Bina Nusantara University, Jakarta, Indonesia

DOI: http://dx.doi.org/10.15294/pandecta.v15i2.18293

Article info

Article History:
Received : January 30td 2020
Accepted: August 15td 2020
Published: December 1st 2020

Keywords:
sovereignty;
cyber;
digital sovereignty

Abstrak

Perkembangan TIK, khususnya internet, memunculkan berbagai aktivitas melalui ruang siber (cyberspace) yang memunculkan manfaat dan resiko secara bersamaan. Dalam perspektif negara, pemanfaatan TIK dapat dioptimalkan untuk menjalankan fungsi negara dalam mewujudkan kesejahteraan masyarakat. Guna mendorong pemanfaatan dalam ruang siber secara optimal, diskusi mengenai kedaulatan negara dalam ruang siber menjadi salah satu pertanyaan mendasar. Penegakan kedaulatan digital oleh negara kerap pula diperlukan untuk meminimalisasi efek negatif yang timbul pada lingkup politik, sosial, ekonomi, budaya dan keamanan nasional. Olehkarenanya, penelitian ini bertujuan untuk melihat bagaimana kedaulatan digital diinterprestasikan oleh Indonesia melalui instrumen pemerintahan. Penelitian ini merupakan penelitian tahap awal yang memerlukan penelitian lanjutan. Menggunakan metode yuridis normatif, penelitian awal ini menyimpulkan bahwa dalam rangka pembentukan kedaulatan digital oleh negara, Indonesia saat ini memusatkan pada pembentukan cyber territory dan sumber daya manusia sebagai langkah awal untuk membangun kedaulatan digital. Namun, Indonesia belum memiliki regulasi pada level undang-undang yang secara khusus mengatur mengenai perlindungan data pribadi.

Abstract

The development of ICT's, especially the internet, has led to various activities through cyberspace that has generated benefits and risks simultaneously—from a state's perspective, using ICTs to carry out the state's function in externalizing the welfare's society. To optimize cyberspace's utilization, the discussion on state sovereignty in cyberspace is one of the fundamental questions. The state's enforcement of digital sovereignty is often needed to minimize the adverse effects on political, social, economic, cultural, and national security. Therefore, this research goal is to analyze how Indonesia interprets digital sovereignty through government instruments. This research is early-stage research that requires further research. This preliminary study concludes that Indonesia is currently focusing on developing cyber territory and human resources as a first step to develop Indonesia's digital sovereignty. However, the protection of personal data has not been covered by a specific personal data act at this moment.
Siber; kedaulatan; kedaulatan digital
sovereignty; cyber; digital sovereignty

✉
Address : Jl. Kemanggisan Ilir III No. 45, Palmerah
Jakarta 11480, Indonesia
E-mail : syuniarti28@gmail. com

ISSN 1907-8919 (Cetak)
ISSN 2337-5418 (Online)

1. Pendahuluan

Era digital yang dilahirkan dari perkembangan teknologi informasi, khususnya internet, membawa manusia ke dalam revolusi informasi yang melahirkan dunia baru berbentuk virtual, dunia siber (*cyber world*). Perkembangan komputer yang didukung oleh perkembangan teknologi informasi dan komunikasi melahirkan jaringan komputer sebagai cikal bakal internet yang memungkinkan penggunanya untuk saling bertukar data dan informasi melalui aktivitas dalam dunia siber. Aktivitas dalam dunia siber yang berbentuk virtual melahirkan suatu interaksi secara global dengan karakteristik meniadakan batas ruang (*boarderless*) dan waktu.

Efektivitas dan efisiensi merupakan beberapa manfaat dari penggunaan internet sehingga penggunaannya semakin massif dan beragam sejak kemunculannya pada proyek ARPANET (*Advance Research Project Agency*) di sekitar tahun 1960. Di sisi lain, aktivitas dalam ruang siber juga menimbulkan problematika dan ancaman siber dalam bentuk kesalahan komputer*, cyber exploitation* atau *cyber attack* yang merupakan risiko baru yang membahayakan jiwa dan milik(Hollis, 2012, p. 2). Problematika yang muncul tidak hanya berdampak pada individu sebagai bagian dari masyarakat, namun berdampak pula pada kedaulatan suatu negara.

Kedaulatan merupakan kekuasaan tertinggi negara yang diturunkan dalam hak-hak berdaulat (*sovereignty rights*) yang merupakan hak dimiliki hanya oleh negara(Adolf, 2015, p. 2). Hans Kelsen mengambarkan konsep tersebut melalui adigium *Qui in territorio meo est,estiam meus subditus est* (jika seseorang berada di wilayah saya, maka ia juga tunduk pada saya)(Adolf, 2015, p. 15). Menurut Bob Barr, kedaulatan nasional terancam apabila suatu negara yang memiliki kekuasaan dan regulasi mendapat ancaman gangguan dari pihak asing(Obar & Clement, 2013, p. 1).

Kasus penyadapan oleh Amerika Serikat dan aliansinya terhadap pejabat negara-negara lain yang diungkap oleh Edward Snowden merupakan salah satu contoh ancaman kedaulatan dari luar negara. Tercatat beberapa kali Indonesia mengalami serangan dalam *cyber war* (Sa'diyah, 2016, p. 169). Berdasarkan laporan tahunan *Honeynet project* 2019, jumlah serangan siber yang ditujukan pada Indonesia adalah sebesar 98.243.896 serangan(Badan Siber dan Sandi Negara, 2019, p. 9). Dari sisi internal, isu-isu SARA maupun konten negatif lainnya dengan mudah didistribusikan melalui media sosial, lemahnya literasi digital meningkatkan jumlah *hoax* dan penyebaran ujaran kebencian (*hate speech*). Tercatat pengaduan yang diterima Polda Metro Jaya aduan terkait ujaran kebencian (*hate speech*) pada tahun 2017 adalah 3.325 laporan, naik 44,99% dari tahun 2016(Medistiara, n.d.). Kerugian yang timbul dari kejahatan siber, terutama *e-commerce,* setiap tahunnya mencapai USD 1,5 triliun(Fahlevi, Saparudin, Maemunah, Irma, & Ekhsan, 2019, p. 5).

Konsep kedaulatan dalam dunia siber diterjemahkan dalam beragam bentuk model pengaturan oleh masing-masing negara. Cina merupakan salah satu negara yang menggunakan model pengaturan berdasarkan kedaulatan dengan prioritas kontrol ada pada negara. Kedaulatan digital yang dikembangkan oleh Cina merupakan bagian dari keamanan informasi yang fokus pada kontrol dan manajemen internet dan konten(Schia & Gjesvik, 2017, p. 1). Beberapa negara di kawasan Asia, Afrika dan Timur Tengah memberlakukan restriksi ketat di internet seperti dilakukan oleh Pemerintah Iran dengan memblokir situs-situs web berbahasa inggris BBC dan *Voice of America* dan mengalihkan penelusuran ke situs-situs website yang memuat nilai-nilai revolusi Iran(Atmaja, 2014, p. 51). Sedangkan, model pengaturan lain yang diikuti oleh Amerika Serikat dan Inggris adalah bahwa pengaturan internet tidak dapat sepenuhnya dilakukan oleh negara namun melibatkan banyak pihak seperti organisasi non-pemerintah, akademis, individu(E. Eichensehr, 2015, p. 317) .

Indonesia sebagai bagian dari masyarakat dunia tidak lepas dari perkembangan teknologi informasi. Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia tahun 2018 bahwa jumlah pengguna inter-

net di Indonesia adalah 64,8% persen jumlah penduduk Indonesia(Asosiasi Jasa Penyelenggara Internet Indonesia, 2018, p. 2). Jumlah tersebut akan terus meningkat seiring dengan pembangunan jaringan (*network*) yang akan membuka akses lebih luas terhadap internet. Dengan semakin terbukanya akses terhadap internet, salah satu tujuan utama Indonesia adalah menjadikan *e-commerce* sebagai salah satu tulang punggung ekonomi di masa akan datang. Namun demikian, sebagaimana telah dijabarkan bahwa pemanfaatan internet perlu dibarengi dengan upaya mengantisipasi dampak merugikan yang mungkin timbul, termasuk terhadap kedaulatan negara.

Lebih lanjut, bentuk pemerintahan yang diterapkan di Indonesia menempatkan Presiden sebagai pemegang kekuasaan pemerintahan dengan dibantu oleh menteri. Terkait dengan pengelolaan ruang siber, Kementerian Komunikasi dan Informartika (Kominfo) diserahi tugas penyelenggaraan urusan pemerintahan di bidang komunikasi dan informatika. Pada awal peran Kominfo, Kominfo menangani urusan terkait dengan siber, termasuk pada penanggulan serangan-serangan siber. Selanjutnya, peran Kominfo terkait dengan keamanan siber dilakukan oleh Badan Siber dan Sandi Negara (BSSN) yang merupakan lembaga pemerintah non kementerian yang fokus pada keamanan siber sebagaimana ditetapkan dalam Peraturan Presiden No. 53 Tahun 2017 diubah dengan Peraturan Presiden No. 133 Tahun 2017. Dalam hukum administrasi negara, Pemerintah dalam menjalankan tugas dan fungsinya membutuhkan instrumen pemerintahan. Menurut Ridwan, instrumen pemerintahan merupakan alat-alat atau sarana-sarana yang digunakan oleh pemerintah atau administrasi negara dalam menjalankan tugas-tugasnya, berupa instrumen non yuridis dan instrumen yuridis. Termasuk dalam instrumen yuridis adalah peraturan perundang-undangan, keputusan-keputusan, peraturan kebijakan, perizinan, instrumen hukum keperdataan dan lainnya(Ridwan, 2011, p. 194).

Selanjutnya, melalui instrumen pemerintahan yang digunakan oleh Pemerintah, penelitian ini merupakan penelitian awal yang bertujuan untuk menganalisa arah pembentukan kedaulatan digital Indonesia. Tentunya diperlukan penelitian lanjutan untuk menjawab rumusan masalah utama tersebut, baik dari sisi pengunaan instrumen pemerintahan lainnya maupun institusi lain yang terkait.

2. Metode

Penelitian ini menggunakan metode yuridis normatif yang berfokus pada nilai-nilai, norma dan aturan tertulis. Sebagai penelitian hukum normatif, penelitian ini dilakukan melalui penelusuran regulasi dan tinjauan pustaka yang diklasifikasikan sebagai data sekunder. Pendekatan yang digunakan adalah pendekatan statuta yang berfokus pada regulasi terkait penelitian dan pendekatan konseptual yang berfokus pada konsep-konsep kedaulatan. Data yang dikumpulkan selanjutnya akan dianalisis dengan menggunakan konsep yang digunakan untuk menjawab permasalahan hukum yang timbul dalam penelitian ini

3. Hasil Penelitian dan Pembahasan

Konsepsi Kedaulatan

Terminologi kedaulatan memiliki beragam makna dan penafsiran. Istilah kedaulatan dapat memiliki makna berbeda bagi orang yang berbeda, yang masing-masing memiliki latar belakang beragam pula. Istilah kedaulatan mungkin memiliki makna berbeda dalam ilmu hukum, ilmu politik, sejarah, filsafat dan bidang-bidang lain yang berkaitan dengannya(Riyanto, 2012, p. 6). Menurut *Black's Law Dictionary*, kedaulatan (*sovereignty*) diartikan sebagai "*the freedom of the nation has its correlate in the sovereignity of the nation. Political sovereignty is the assertion of the self-determinate will off the organic people, and in this there is the manifestation of its freedom. It is in and through the determination of its sovereignty that the order of the nation is constituted and maintained*".

Kedaulatan merupakan hal yang membedakan negara dengan subyek hukum lainnya(Adolf, 2015, p. 1). Kedaulatan merupakan ciri atau atribut yang bersifat khusus bagi negara(Isjwara, 1999, p. 108).

Kedaulatan-lah yang membuat negara dilihat sebagai sebuah entitas yang otonom dan independen(Kusumawardhana & Zulkarnain, 2016, p. 6145). Kaitannya dengan kedaulatan, hukum merupakan aspek yang sangat penting. Kristalisasi hubungan hukum dan kedaulatan dikemukan oleh Jean Bodin yang mengemukakan bahwa kedaulatan merupakan sumber utama untuk menetapkan hukum. Kedaulatan merupakan sumber otoritas yang berada pada aras tertinggi hirarki hukum (*legal hierarchy*)(Riyanto, 2012, p. 7). Menurut Mochtar Kusumaatmadja, untuk menjalankan fungsi hukum, hukum memerlukan kekuasaan, tetapi kekuasaan itu sendiri harus berjalan dalam batas dan rambu-rambu yang ditentukan oleh hukum itu sendiri(Atmasasmita, 2012, p. 7).

Kekuasaan dalam konteks hukum berkaitan dengan kekuasaan negara. Struktur kekuasaan negara bersifat hierarkis atau berjenjang, mulai dari kekuasaan tertinggi sampai kekuasaan terendah. Kekuasaan tertinggi dalam suatu negara adalah kedaulatan(Hanoraga, 2008, p. 56). Pengertian mendasar dari kedaulatan diartikan sebagai kekuasaan untuk membuat dan melaksanakan undang-undang dengan segala cara pemaksaan yang diperlukan(Irawan, 2018, p. 19).

Menurut Milton J. Esman, ada 2 (dua) dimensi pelaksanaan kedaulatan setiap negara, yaitu pelaksanaan kedaulatan ke dalam (*internal sovereignty*) yang mencakup perilaku orang dan kontrol atas sumber daya dalam wilayah teritori negara; dan (2) dimensi pelaksanaan kedaulatan keluar (*external sovereignty*) yang membatasi pertemuan (*interface*) oleh pihak luar dalam urusan domestik kecuali diijinkan secara sukarela oleh pemerintah(Purna Cita Nugraha, 2013, p. 42). Lebih lanjut, Jimmy Asshiddiqie menerangkan bahwa konteks kedaulatan dalam arti internal merujuk pada konsep kekuasaan tertinggi yang dikenal selama ini dalam dunia filsafat hukum dan politik mencakup ajaran tentang kedaulatan Tuhan (*theocracy*), kedaulatan rakyat (*democracy*), kedaulatan hukum (*nomocracy*), dan kedaulatan raja (*monarchy*). Dalam perspektif eksternal, konsep kedaulatan itu biasa dipahami dalam konteks hubungan antar negara(Asshiddiqie, 2009, p. 1).

Kedaulatan Digital

Terminologi kedaulatan digital muncul seiring dengan perkembangan teknologi informasi dan komunikasi, khususnya internet. Menurut Kamus Besar Bahasa Indonesia, Internet merupakan jaringan komunikasi elektronik yang menghubungkan jaringan komputer dan fasilitas komputer yang teroraganisasi di seluruh dunia melalui satelit atau telepon. *International Telecomunication Union* (ITU) mendefinisikan internet sebagai "*a collection of interconnected network using the Internet Protocol which allows them to function as a single, large virtual network".*Adapun The Federal Networking Council (FNC) menyebutkan bahwa *internet refers to the global information system that- (a) is logically linked together by a globally unique address space based on the Internet Protocol* (IP) *or its subsequent extension/follow-ons; (b) is able to support communication using the transmission control protocol/internet protocol (TCP/IP) suite or its subsequent extension/follow-ons, and/or other IP-compatible protocols;and* (iii) *provides, uses or makes accessible, either publicly or privately high level service layered on the communication and related infrastructure describe herein"*. Sedangkan, *The American Supreme Court* mengklasifikasikan internet sebagai "*a unique and wholly new medium of worldwide communication taken together, these tools (email, mailing list servers, newsgroups, chat rooms, world wide web) constitue a unique new medium-known to its users as cyberspace,located in no particular geographical location but available to anyone, anywhere in the world with access to the internet"*(Proksch & Schweighofer, 2011, p. 2). Setidaknya benang merah dari ketiga definisi tersebut menyebutkan bahwa pada dasarnya internet merupakan sebuah media komunikasi.

Terminologi "kedaulatan digital" diberikan definisi oleh Piere Belangger pada sekitar tahun 2000, sebagai:*"digital soveregnity is a control of our present and destiny as manifested and guided by the use of technology and*

computer network"(Gueham, 2017, p. 9). Dari perspektif industri, *digital sovereignity is the capability of a natural person or corporate entity for exclusive self determination with regard to its economic data goods* (Scerri, 2016, p. 10). Dalam perspektif *cybersecurity,* kedaulatan dipersepsikan sebagai kedaulatan atas data(Nugraha, Kautsarina, & Sastrosubroto, 2015, p. 1).Menurut Hao Yeli, kedaulatan dalam ruang siber (*cyber sovereignty*) dalam perspektif *cybersecurity* masih menjadi perdebatan, yakni: (a) kontradiksi dengan semangat dari internet; (b) kontradiksi dengan hak asasi manusia; dan (c) kontradiksi dengan keterlibatan *multi stakeholders* dalam pengaturan internet. Olehkarenanya, untuk membahas konsep kedaulatan dalam ruang siber perlu dilihat dari 3 (tiga) perspektif pelaku yang terlibat, yakni negara, warganegara (*citizen*) dan komunitas internasional(Hao yeli, 2017, pp. 109–110). Dengan demikian pengertian atas kedaulatan digital merujuk pada makna berbeda dilihat dari perspektif yang digunakan.

Pembahasan mengenai kedaulatan digital pada dasarnya mendiskusikan pengaturan negara atas ruang siber. John Perry Barlow dalam *a declaration of the independence of cyberspace* menyatakan bahwa ruang siber memberikan kebebasan kepada individu dan intervensi negara adalah suatu hal yang tidak diperlukan(Barlow, 1996). Pierre Bellanger mengilustrasikan posisi negara dan internet yang mana negara adalah tempat sedangkan internet adalah sebuah tautan (*link*). Kedaulatan muncul pada tempat/wilayah, sedangkan internet menghubungkan keseluruhan wilayah tersebut menjadi satu. Internet ibarat lautan yang menghubungkan berbagai wilayah tanpa menjadi bagian dari wilayah tersebut(Gueham, 2017, p. 3). Namun demikian, pada akhirnya internet sebenarnya bukan merupakan suatu ruang yang tanpa pengaturan. Dalam konteks internet, pengaturan negara ditujukan kepada *behaviour* warga ketika berada dalam suatu jaringan (*net*)(Lawrence, 2006, p. 38).

Pengaturan oleh negara kerap dikaitkan dengan konsep kedaulatan. Konsep kedaulatan identik dengan wilayah sebagai teritori dimana kedaulatan memiliki bentuknya. Dalam ruang siber, batas wilayah merupakan suatu hal yang tak muncul. Apabila mengkaitkan konsep kedaulatan dengan teritori, maka teknologi informasi telah membuat konsep wilayah itu juga mengalami metamorfosa(Kusumohamidjojo Budiono, 2016, p. 86). Bahkan Menthe mendefinisikan ruang siber sebagai ruang virtual yang harus diperlakukan seperti ruang internasional lainnya (antartika, alam semesta, atau lautan) (Jiménez & Lodder, 2015, p. 269). Namun demikian, konsepsi kedaulatan sebagai suatu hal yang tidak dapat dibagi perlu ditelaah kembali dalam kontek globalisasi yang mana hubungan antar negara menjadi lebih kompleks dan rumit, tanpa meruntuhkan nilai dari kedaulatan itu sendiri(Purna Cita Nugraha, 2013, p. 43)

Terlepas dari perdebatan mengenai hal tersebut, secara aktual, negara-negara telah memiliki regulasi terkait aktivitas ruang siber. Melalui regulasi, negara memiliki kewenangan untuk mengatur aktivitas ruang siber. Pada dasarnya secara yuridis konsep wewenang (*authority*) selalu berkaitan dengan kekuasaan (*power*) yang berdasarkan hukum, baik cara perolehannya maupun cara penggunaanya(Rokhim, 2013, p. 137). Kehadiran hukum menjadi diperlukan karena walaupun aktivitas dalam ruang siber dilakukan secara virtual, namun warga pada jaringan (*net*) merupakan masyarakat yang berasal dari dunia nyata dan walaupun terjadi di dunia virtual, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata(Sitompul, 2012, p. 39).

Kedaulatan Digital Indonesia

Menjadi negara yang berdaulat tercantum secara tegas dalam Pembukaan UUD 1945. Pada Manifesto TIK 2045 yang disusun oleh Badan Litbang SDM Kominfo, TIK merupakan penjaga kedaulatan dan kepentingan nasional pada sistem geopolitik dan ekonomi lokal(Badan Litbang SDM Kominfo, 2016, p. 27). Menjaga kedaulatan juga merupakan salah satu tujuan dalam Rencana Pembangunan Jangka Panjang Nasional periode 2005-2025. Globalisasi dan revolusi teknologi informasi dalam Rencana Pembangunan

Jangka Panjang Nasional 2005-2025 diakui merupakan tantangan sekaligus peluang bagi Indonesia yang secara geografis merupakan negara kepulauan, multi etnis dengan demografi penduduk yang besar. Globalisasi, demokrasi dan inovasi teknologi terutama perkembangan TIK memungkinkan informasi mengalir bebas dan tidak mengenal batas negara.

Lebih lanjut, dalam Rencana Pembangunan Jangka Panjang Nasional 2005-2025, khusus mengenai pembangunan pos dan telematika dilakukan melalui penciptaan landasan kompetisi dalam lingkungan multioperator, antisipasi implikasi TIK, baik mengenai kelembagaan maupun peraturan mengenai isu keamanan, kerahasiaan, privasi dan integritas informasi; penerapan hak kekayaan intelektual, peningkatan legalitas, pembangunan infrastruktur dan prasarana jaringan, penerapan konsep teknologi netral, peningkatan pengetahuan masyarakat, pengembangan industri dalam negeri dan industri konten sebagai upaya penciptaan nilai tambah dari informasi. Komponen dari pembangunan TIK dalam rangka mencapai visi Indonesia 2025, adalah: (a) migrasi menuju konvergensi; (b) pemerataan akses dan layanan;(c) pengembangan jaringan pita lebar; (d) peningkatan keamanan dan jaringan sistem informasi; (e) integrasi infrastruktur, aplikasi dan data nasional; (f) peningkatan e-literasi, kemandirian industri TIK domestik dan SDM TIK siap pakai;dan (g) peningkatan kemandirian industri TIK dalam negeri.

Walaupun internet telah digunakan sejak sekitar tahun 1990-an, ketentuan yang khusus mengatur aktivitas siber baru memiliki legalitas formal pada tahun 2008 melalui Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang No. 9 Tahun 2016 (UU ITE). UU ITE dibentuk dengan suatu pemahaman bahwa masalah-masalah yang timbul dari aktivitas dalam ruang siber tidak dapat digunakan dengan menggunakan pranata hukum konvensional.Secara eksplisit dinyatakan dalam UU ITE bahwa tiga aspek yang digunakan untuk menjaga keamanan ruang siber yang dilakukan oleh Indonesia,yakni aspek hukum, aspek teknologi dan aspek sosial, budaya dan etika. Pembentukan UU ITE juga sebagai bagian dari upaya memberikan kepastian hukum, karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Efektifitas waktu dalam proses penerbitan aturan serta untuk memastikan keterkaitan materi-materi secara komprehensif sebagai pertimbangan, UU ITE dibuat dengan lingkup pengaturan yang luas(Kementerian Komunikasi dan Informatika, 2009, p. 9), mulai dari ketentuan terkait transaksi elektronik sampai dengan hal-hal yang dilarang dilakukan dengan ancaman pidana penjara dan denda. Ada 3 aturan pelaksana yang diamanatkan dalam UU ITE, yakni: (1) Peraturan Pemerintah mengenai Penyelenggaraan Informasi dan Transaksi Elektronik; (2) Peraturan Pemerintah megenai Tata Cara Intersepsi; (3) Peraturan Pemerintah mengenai Data Elektronik Strategis. Saat ini, peraturan pelaksana mengenai penyelenggaraan informasi dan transaksi elektronik dituangkan dalam Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE"). Adapun Pasal 31 ayat (4) UU ITE yang mengamanatkan adanya Peraturan Pemerintah mengenai Tata Cara Intersepsi dibatalkan keberlakuannya berdasarkan Putusan Mahkamah Konstitusi No.5/PUU-VIII/2010. Sejak UU ITE diundangkan, telah diajukan uji materiil kepada Mahkamah Konstitusi seperti pada Tabel 1.

Dunia siber tidak diberikan arti secara definitif dalam UU ITE, selain dalam penjelasan dalam UU ITE sebagai kegiatan melalui media sistem elektronik. Dalam putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008 dinyatakan bahwa aktivitas-aktivitas di dunia siber mempunyai karakter, yaitu: (1) mudah, (2) penyebarannya sangat cepat dan meluas yang dapat diakses oleh siapapun dan dimanapun, dan (3) dapat bersifat destruktif dari pemuatan materi penghinaan dan/atau pencemaran nama baik dengan menggunakan media elektronik sangat luar biasa karena memiliki corak viktimisasi yang tidak terbatas. Olehkarenanya, pembeda utama

Tabel 1. Uji Materiil UU ITE

Putusan Mahkamah Konstitusi	Ketentuan UU ITE		Putusan
50/PUU-VI/2008	Pasal 27 ayat (3) Pasal 45 ayat (1)	Pencemaran nama baik	Ditolak
2/PUU-VII/2009	Pasal 27 ayat (3)	Pencemaran nama baik	Tidak dapat diterima
5/PUU-VIII/2010	Pasal 31ayat (4)	Intersepsi	Diterima
52/PUU-XI/2013	Pasal 28 ayat (2)	Penyebaran informasi yang menimbulkan rasa kebencian	Ditolak
20/PUU-XVI/2016	Pasal 5 ayat (1) dan (2),Pasal 44 huruf (b)	Alat bukti elektronik	Dikabulkan sebagian
76/PUU-XV/2017	Pasal 28 ayat (2);Pasal 45A ayat (2)	Penyebaran informasi yang menimbulkan rasa kebencian	Ditolak

antara interaksi di dunia nyata (*real/physical world*) dan dunia maya (*cyberspace*) hanyalah dari sudut media yang digunakan.

Secara terminologi, dalam UU ITE tidak ditemukan kata "kedaulatan" selain pada penjelasan Pasal 2 UU ITE terkait dengan lingkup "merugikan kepentingan Indonesia" sebagai unsur keberlakuan UU ITE. Konsep kedaulatan muncul pada Pasal 2 UU ITE melalui penegasan bahwa keberlakuan ketentuan dalam UU ITE merujuk pada akibat dan kerugian dari perbuatan, tidak melihat apakah perbuatan tersebut dilakukan di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia. Kerugian dimaksud adalah kerugian terhadap kepentingan Indonesia, yang tidak hanya terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, warga negara serta badan hukum Indonesia, namun juga meliputi kedaulatan negara. Ancaman hukuman juga diberikan terhadap tindakan-tindakan dilarang dalam Pasal 27 sampai dengan Pasal 36 UU ITE yang dilakukan di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah Indonesia.

Lebih lanjut, dalam pemanfaatan teknologi dan informasi, secara eksplisit Pemerintah menempatkan posisi sebagai fasilitator sebagaimana dinyatakan dalam Pasal 40 ayat (1) UU ITE. Sebagai fasilitator, arah regulasi, kebijakan dan tindakan Pemerintah merujuk pada berbagai upaya untuk memfasilitasi pemanfaatan TIK. Salah satu bentuk pemanfaatan teknologi dan informasi yang menjadi target Pemerintah adalah *e-commerce* sebagai salah satu tulang punggung ekonomi Indonesia sebagaimana dinyatakan dalam Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik yang kemudian ditindaklanjuti dengan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Berbagai program disusun Pemerintah untuk mendorong perkembangan *start-up* dalam ekosistem ekonomi digital Indonesia, antara lain melalui Gerakan Nasional 1000 start up digital(Kementerian Komunikasi dan Informatika, 2016), mendorong kehadiran *decacorn*(Kementerian Komunikasi dan Informatika, 2019a), UMKM go online (Kementerian Komunikasi dan Informatika, 2019c).

Pembahasan kedaulatan digital Indonesia kerap menjadi kajian yang diikuti dengan usulan rumusan hal-hal yang perlu dimiliki oleh Indonesia untuk mewujudkan kedaulatan digital tersebut. Pada *Roadmap* TIK 2016-2045, diakui bahwa kedaulatan negara saat ini adalah dalam bentuk kedaulatan siber. Kedaulatan siber ditempatkan dalam perspektif negara harus memiliki kekuasaan dan kemampuan untuk mengatur serta mengawasi lalu lintas internet domestik maupun global di pintu gerbang keluar/masuk

wilayah siber negara tersebut(Badan Litbang SDM Kominfo, 2016, p. 26). Menurut Masyarakat Telekomunikasi Indonesia (MASTEL), kedaulatan siber dapat meliputi: (a) keamanan dan kenyamanan siber warga negara; (b) kewajaran penguasaan ekonomi lokal; (c) melindungi *critical infrastruktur* Pemerintah; (d) mengendalikan penetrasi ideologi, politik, sosial dan budaya; dan (e) melindungi warga negara (*privacy* dan data) dan anak-anak. Untuk menjaga kedaulatan siber, MASTEL mengusulkan terlebih dahulu penetapan lingkup yang harus dijaga (ragam territorial wilayah siber), mengklasifikasikan tindakan pencegahan dan penanggulangan serta menetapkan instrumen yang diperlukan(Masyarakat Telematika Indonesia, 2015, pp. 5–6). Adapun dalam perspektif *cybersecurity,*menurut Nugraha Kautsarina & Sastrosubroto adalah pembentukan kedaulatan data (*data sovereignty*) Indonesia dengan fokus pada kerahasiaan data (*data confidentiality*), keutuhan data (*data integrity*) dan keberadaan data (*data avalaibility*)yakni melalui enkripsi, layanan email nasional, lokalisasi pusat data (*data center*), *routing* nasional pada trafik internet, infrastruktur *backbone* jaringan telekomunikasi nasional(Nugraha et al., 2015, p. 1).

Pada *Roadmap* TIK 2016-20145 yang disusun oleh Badan Litbang SDM Kominfo, kedaulatan digital Indonesia diinterprestasikan dalam bentuk kendali negara terhadap akses entitas dan aktivitas internet dalam wilayah Indonesia. Untuk itu, diperlukan penetapan wilayah siber Indonesia (*cyber territory*) yang dilakukan dengan menata konfigurasi jaringan *broadband* domestik (jaringan pita lebar) dan membangun gerbang pembatas antara jaringan *broadband* global dan nasional/domestik. Melalui pembatasan tersebut, negara dapat mengontrol jaringan domestik dan global yang terkoneksi dengan gerbang nasional Indonesia. Dengan pembentukan *cyber territory,* negara menerapkan kedaulatan melalui pembentukan Gerbang Internet Nasional (*Internet National Gateway*), sebagai pintu keluar masuk informasi dalam wilayah *cyber territory* Indonesia serta penempatan data center di dalam wilayah Indonesia(Badan Litbang SDM Kominfo, 2016, pp. 26–27). Lebih lanjut, berdasarkan *Roadmap* TIK 2016-2045 tersebut, *output* yang dihasilkan pada tahun 2045 adalah: (a) *cyber teritory* Indonesia; (b) sumber daya ma-

Tabel 2. Roadmap TIK Indonesia 2016-2045

Sasaran	Aspek	Kata Kunci	Program
Indonesia Berdaulat	Kedaulatan siber Indonesia	Infrastruktur	Intranet Indonesia, cloud pemerintah dan layanan publik, membangun intranet pemerintah dan data center lokal, internet masyarakat via gateway, pemerintah dan masyarakat menggunakan internet (global) dengan layanan publik menerapkan NSID
Indonesia Mandiri	Industri Mandiri	Internet, aplikasi, konten dan digitalisasi	industri apps dan konten (termasuk apps IoT) dengan server dan intranet Indonesia, industri glokal apps lintas negara yang afirmatif dengan national payment gateway, serta server ZIPCode dan NSID untuk batas virtual dan layanan publik.
Indonesia Sejahtera	Rakyat Sejahtera	SDM dan social readiness	penguasaan teknologi dan pasar TIK global, cooperative and community-based apps developer networks, civil society platform untuk perlindungan masyarakat.

Sumber: (Badan Litbang SDM Kominfo, 2016, p. 23)

nusia sebagai penjaga teritori; (c) manufaktur infrastruktur dan perangkat; (d) gerbang internet Indonesia; (e) politik luar negeri/globalisasi online(Badan Litbang SDM Kominfo, 2016, pp. 29–30) (Kominfo,2016:29-30).

Melalui instrumen pemerintahan yang digunakan oleh Pemerintah, berikut adalah bentuk pelaksanaan kedaulatan digital oleh Indonesia saat ini:

a. Kontrol terhadap konten

Pelaksanaan kedaulatan dilaksanakan dalam bentuk peran negara untuk melindungi kepentingan umum. Melalui Pasal 40 ayat (2) UU ITE, Pemerintah melindungi ketertiban umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan transaksi elektronik yang menggangu ketertiban umum. Lebih lanjut, dibebankan pula kewajiban bagi Pemerintah untuk mencegah penyebarluasan dan penggunaan informasi dan/atau dokumen elektronik tersebut. Untuk itu Pemerintah diberikan kewenangan melalui Pasal 40 ayat (2.b) UU ITE untuk melakukan pemutusan akses, baik yang dilakukan langsung oleh Pemerintah maupun penyelenggara sistem elektronik.

Namun demikian, klasifikasi jenis gangguan yang dianggap menganggu ketertiban umum tersebut tidak diatur lebih lanjut dalam UU ITE. Sebelum berlakunya PP PSTE, pemutusan akses dilakukan melalui Peraturan Menteri Komunikasi dan Informatika No. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif ("Permenkominfo No.19/2014") yang memberikan klasifikasi situs internet bermuatan negatif , yakni jenis situs internet yang memuat pornografi dan kegiatan ilegal lainnya berdasarkan ketentuan perundang-undangan. Setelah diterbitkannya PP PSTE, pemutusan akses dapat dilakukan apabila: (1) melanggar ketentuan peraturan perundang-undangan; (2) meresahkan masyarakat dan menganggu ketertiban umum seperti informasi dan/atau fakta yang dipalsukan; dan (3) memberitahukan atau menyediakan akses terhadap informasi dan/atau dokumen elektronik yang melanggar perundang-undangan. Adapun dimaksud dengan melanggar ketentuan peraturan perundang-undangan meliputi antara lain mengandung unsur- unsur: (1) perbuatan yang dilarang dalam UU ITE, yakni mengandung unsur pornografi, fitnah dan/atau pencemaran nama baik, penipuan, kebencian terhadap suku, agama, ras dan antar golongan, kekerasan dan/atau kekerasan anak, pelanggaran kekayaan intelektual; (2) pelanggaran perdagangan barang dan jasa melalui sistem elektronik; (3) terorisme dan/atau radikalisme, separatisme dan/atau organisasi berbahaya terlarang; (4) pelanggaran keamanan informasi; (5) pelanggaran perlindungan konsumen, bidang kesehatan, pengawasan obat dan makanan.

.Penyaringan konten negatif dilakukan secara rutin oleh Ditjen Aplikasi Informatika dengan menggunakan aplikasi TRUST+Positif. Sistem TRUST+Positif menerapkan mekanisme kerja adanya server pusat yang akan menjadi acuan dan rujukan kepada seluruh layanan akses informasi publik (fasilitas bersama) serta menerima informasi-informasi atas fasilitas akses informasi publik untuk menjadi alat analisa dan profiling penggunaan internet di Indonesia(Kementrian Komunikasi dan Informatika, 2013). Saat ini, TRUST+Positif digantikan dengan mesin pengais konten negatif (AIS) sebagai mesin berbasis *crawling*(Kementrian Komunikasi dan Informatika, 2018b).

Selain, penelusuran konten negatif dengan menggunakan aplikasi, pemblokiran dilakukan pula berdasarkan laporan masyarakat. Laporan masyarakat dianggap mendesak dalam hal terkait dengan: (1) privasi; (2) pornografi; (3) kekerasan; (4) suku agama, ras dan antargolongan; dan/atau (5) muatan lainnya yang berdampak negatif yang menjadi keresahan masyarakat secara luas. Dalam hal pemblokiran telah dilakukan, pengelola situs atau masyarakat dapat mengajukan normalisasi atas pemblokiran situs.

Kontrol terhadap konten juga dilakukan oleh Kominfo melalui penyelenggara sistem elektronik. Sebagai pengelola sistem, penyelenggara sistem elektronik memiliki otoritas dan kemampuan untuk melakukan rekayasa arsitektur sistem elektronik yang berada dalam pengelolaanya. Hal tersebut dapat dipahami dengan memahami esensi dari

internet sebagai suatu jaringan. Tercatat Kominfo memblokir aplikasi *Telegram* melalui pemblokiran 11 *domain name system* Telegram. Pemblokiran dilakukan karena adanya konten bermuatan radikalisme dan terorisme yang beredar melalui Telegram(Kementerian Komunikasi dan Informatika, 2017).

b. Kontrol terhadap data

Dalam pidato kenegaraan Presiden di depan Sidang DPR/MPR pada tanggal 16 Agustus 2019 disebutkan bahwa kedaulatan atas data harus diwujudkan hak warga negara atas data pribadi harus dilindungi. Berdasarkan penelitian Lembaga Studi dan Advokasi Masyarakat (ELSAM), setidaknya ada 30 (tiga puluh) undang-undang di Indonesia yang menyebutkan mengenai perlindungan data pribadi(Wahyudi & Sumigar Bernhard Ruben Fritz, 2016, pp. 30–31). Namun demikian, ketentuan perundang-undangan yang secara khusus mengatur mengenai perlindungan data pribadi sebatas rancangan undang-undang data pribadi.

UU ITE menempatkan persetujuan sebagai dasar penggunaan data pribadi seseorang, kecuali ditentukan lain oleh perundang-undangan. Lebih lanjut, berdasarkan penetapan pengadilan, seseorang dapat mengajukan permintaan penghapusan data dirinya yang tidak relevan kepada penyelenggara sistem elektronik. Dari sisi teknis, perlindungan data dilakukan dengan pembebanan serangkaian tanggungjawab kepada penyelenggara sistem elektronik guna melindungi data pribadi, seperti perolehan dan pengungkapan harus seijin pemilik data, kewajiban menyampaikan informasi kepada pengguna mengenai jaminan privasi dan.atau perlindungan data, kategori perlindungan data dalam sertifikat keandalan yang diatur dalam PP PTSE, Peraturan Menteri Komunikasi dan Informatika No. 20/2016 tentang Perlindungan Data Dalam Sistem Elektronik serta peraturan lingkup sektoral.

Data pribadi didefinisikan dalam PP PSTE sebagai setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau non-elektronik. Perlindungan data pribadi dalam sistem elektronik dilakukan pada proses:(a) perolehan dan pengumpulan;(b) pengolahan dan penganalisisan;(c) penyimpanan;(d) perbaikan dan pembaruan; (e) penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; serta (e) pengungkapan dan pemusnahan. Pemrosesan data pribadi pada setiap tahap tersebut merujuk pada prinsip-prinsip perlindungan data pribadi sebagaimana diuraikan dalam PTSE. Lebih lanjut, terkait dengan penempatan pusat data *(data center*) yang semula berdasarkan Peraturan Pemerintah No.80/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik wajib ditempatkan di dalam negeri bagi penyelenggara sistem elektronik untuk pelayanan publik, ditiadakan dalam PP PTSE sebagai pengganti dari PP No.80/2012.

c. Pembangunan Infrastruktur

Dalam rencana pembangunan TIK, kedaulatan siber dilakukan dengan penentuan terlebih dahulu *cyber territory* melalui penataan pita lebar (*broadband*) dan gerbang internet nasional. Pada Rencana Pembangunan Jangka Panjang Nasional 2005-2025, terbatasnya kapasitas, kualitas dan jangkauan diakui menyebabkan timbulnya kesejangan digital. Oleh karenanya, pembangunan di sektor komunikasi adalah pembangunan infrastruktur guna memperluas akses. Untuk itu, Pemerintah membangun konektivitas nasional, salah satunya adalah dengan mengintegrasikan jaringan pita lebar, sebagai salah satu komponen TIK, dengan 3 (tiga) elemen konektivitas lainnya yakni Sistem Logistik Nasional, Sistem Transportasi Nasional dan Pengembangan Wilayah. Pembangunan pita lebar tidak hanya diarahkan untuk kepentingan ekonomi tetapi juga ke seluruh aspek pembangunan, termasuk pertahanan dan keamanan. Pemerintah membuat rencana pembangunan pita lebar (*broadband*) periode 2014-2019 melalui Peraturan Presiden No. 96 Tahun 2014 tentang Rencana Pita Lebar Indonesia 2014-2019. Pita lebar (*broadband*) dalam Pepres No. 96/2014 diartikan sebagai akses internet dengan jaminan konektivitas yang selalu tersambung, terjamin

ketahanannya dan keamanan informasinya serta memiliki kemampuan *triple-play* dengan kecepatan minimal 2 Mbps untuk akses tetap dan 1 Mbps untuk akses bergerak. Pita lebar menjadikan peyediaan, pegolahan dan pendistribusian informasi dilakukan secara lebih cepat, efisien, efektif, transparan dan akuntabel.

Pembangunan pita lebar diarahkan untuk mendorong pertumbuhan ekonomi dan daya saing nasional serta meningkatkan kualitas hidup masyarakat. Program unggulan yang dilakukan guna mendukung penyediaan pita lebar sebagaimana dinyatakan dalam Pepres No. 96/2014, adalah: (a) konektivitas ekonomi, terdiri atas Proyek Ring Palapa, Pipa Bersama, dan Proyek Percontohan Konektivitas Nirkabel untuk pita lebar pedesaan; (b) konektivitas pemerintah dalam bentuk jaringan dan pusat data pemerintah terpadu; (c) pendorong (*enabling*) yang terdiri atas reformasi dana kewajiban pelayanan universal (*universal service obligation*) serta pengembangan sumber daya industri TIK nasional.

Palapa Ring jaringan kabel serat optik sepanjang 2.995kilometer dibangun melintasi Propinsi Kalimantan Timur, Sulawesi Utara, Sulawesi Tengah, Sulawesi Tenggara dan Maluku Utara terdiri atas kabel darat sepanjang 1.326,22 km kabel darat dan 1,787,06 km kabel laut. Melalui proyek Palapa Ring ini memungkinkan akses kecepatan internet 4G sampai dengan 30 Mbp. Sebagai infrastruktur tulang punggung jaringan telekomunikasi *broadband* (pita lebar), Palapa Ring terdiri dari tiga paket, yaitu Palapa Ring Paket Barat, Palapa Ring Paket Tengah dan Palapa Ring Paket Timur yang menghubungkan seluruh Indonesia dalam jaringan telekomunikasi(Kementerian Komunikasi dan Informatika, 2019b).

Guna pengadaan sarana dan prasarana TIK, Kominfo menetapkan ketentuan mengenai pelaksanaan Kebijakan Pelayanan Universal Telekomunikasi dan Informatika (*Universal Service Obligation*). Melalui program ini, Pemerintah melibatkan operator telekomunikasi guna mempercepat pembanguanan sarana dan prasarana pada daerah tertinggal, daerah terpencil, daerah perintisan, daerah perbatasan dan daerah yang tidak layak secara ekonomi sebagaimana diatur dengan regulasi terakhir Peraturan Menteri Komunikasi dan Informatika No. 10 Tahun 2018 tentang Pelaksanaan Kewajiban Universal Telekomunikasi dan Informatika.

d. Penggunaan Aplikasi Lokal dan Peningkatan Sumber Daya Manusia

Penggunaan aplikasi lokal dimaksimalkan melalui persyaratan Tingkat Komponen Dalam Negeri (TKDN) yang ditentukan oleh Pemerintah, khususnya bagi produk telephon seluler, komputer gengam dan komputer tablet. TKDN adalah besarannya komponen dalam negeri pada barang, jasa dan gabungan barang dan jasa. Pada Siaran Pers No.143/HM/KOMFINFO/08/2017, Kominfo berupaya meningkatan penggunaan aplikasi lokal guna membentuk kedaulatan digital.

Secara regulasi, penggunaan tenaga kerja Indonesia wajib digunakan oleh penyelenggara sistem elektronik yang bersifat strategis. Guna peningkatan kualitas sumber daya manusia, Pemerintah melakukan inisiatif untuk melakukan berbagai kerjasama dengan pihak yang terlibat dalam industri TIK dan internet melalui penyelenggaraan pelatihan dan pendidikan bagi sumber daya manusia Indonesia seperti program *Digital Talent Development* bersama perusahaan *big tech company* seperti Microsoft, Cisco, dan Google untuk penguasaan *Cybersecurity, Cloud Computing, Big Data Analytics, Artificial Intelligence*, dan *Digital Business*(Kementerian Komunikasi dan Informatika, 2018) .

Peningkatan sumber daya manusia dilakukan pula dengan pemeringkatan atau akreditasi lembaga pelatihan teknis bidang teknologi informasi dan komunikasi sebagaimana diatur dalam Peraturan Menteri Komunikasi dan Informatika No. 01 Tahun 2018. Akreditasi lembaga pelatihan tersebut bertujuan untuk memberikan penjaminan kelayakan penyelenggaraan pelatihan teknis bidang teknologi, informasi dan komunikasi yang dilakukan melalui serangkaian penilaian terhadap unsur organisasi lembaga pelatihan dan unsur program pelatihan dan pengelo-

laan program pelatihan.

Lebih lanjut, dalam Program Desa *Broadband* terpadu yang menyediakan layanan infrastruktur dan akses layanan informasi (*broadband*) di wilayah non komersial dengan CPR (*Costumer Premise Equipment*) serta konten aplikasi yang produktif dalam pemberdayaan masyarakat, pendampingan sumber daya manusia merupakan bagian dari program desa tersebut. Sempat dihentikan pada tahun 2016, tahun 2017 program Desa *Broadband* terpadu dilaksanakan kembali dengan sasaran Desa 3T untuk memberantas buta internet dan berubah konsep menjadi Solusi Desa *Broadband* Terpadu (SDBT) melalui penyediaan *network, device, application,* dan *capacity building* yang tepat di lokasi sasaran Desa 3T dan Lokasi Prioritas (LokPri) yang dibagi menjadi desa petani, desa nelayan dan desa pedalaman sehingga dapat meningkatkan produktivitas dan memberikan akses ke pasar/*marketplace* agar mendapatkan harga jual terbaik demi meningkatkan kesejahteraannya(Kementrian Komunikasi dan Informatika, 2018a, p. 95).

4. Simpulan

Indonesia, sebagai salah satu negara yang terhubung pada jaringan informasi global, perlu membangun kedaulatan digital untuk mempertahankan kedaulatan negara. Langkah Indonesia dalam pembentukan kedaulatan digital saat ini dilakukan dengan penyiapan infrastruktur berupa pemerataan akses internet ke seluruh wilayah Indonesia melalui proyek Palapa Ring sebagai langkah membentuk *cyber territory* Indonesia. Guna menjaga stabilitas politik, ekonomis, sosial dan budaya, langkah yang ditempuh Pemerintah adalah dengan pemblokiran terhadap konten-konten yang bermuatan negatif. Selain itu, penggunaan aplikasi lokal dan pengembangan sumber daya manusia di bidang siber diperhitungkan sebagai komponen dari pembentukan kedaulatan digital. Namun, perlindungan data masih menjadi pekerjaan rumah dengan belum adanya regulasi setingkat undang-undang yang mengatur secara khusus mengenai perlindungan data. Penelitian lanjutan perlu dilakukan untuk pemetaan lebih komprehensif bagaimana kedaulatan digital diinterprestasikan dan dibangun oleh Pemerintah Indonesia.

5. Daftar Pustaka

Adolf, H. (2015). *Aspek-Aspek Negara Dalam Hukum Internasional* (5th ed.). Bandung: CV Keni Media.

Asosiasi Jasa Penyelenggara Internet Indonesia. (2018). *Laporan Survei Penetrasi & Profil Perilaku Pengguna Internet Indonesia*. *APJI*.

Asshiddiqie, J. (2009). *Gagasan Kedaulatan Lingkungan: Demokrasi Versus Ekokrasi*. https://doi.org/10.1038/132817a0

Atmaja, A. E. (2014). Kedaulatan Negara Di Ruang Maya:Kritik UU ITE Dalam Pemikiran Satipto Rahardjo. *Jurnal Opinio Juris*, *16*(September), 48–91.

Atmasasmita, R. (2012). Tiga Paradigma Hukum Dalam Pembangunan Nasional. *Jurnal Hukum PRIORIS*, *3*(1), 1–26.

Badan Litbang SDM Kominfo. (2016). *Penyusunan Roadmap Pembangunan Sektor TIK Jangka Panjang s . d . 2045 Menuju 100 Tahun Indonesia Merdeka*. (R. W. Harjani Retno Sekar, Aldhino Anggoro Sesar, Eyla Alivia Maranny, Ilhamy Julwendy, Trice Rachmadhani & Kontributor/Narasumber, Eds.). Puslitbang Sumber Daya, Perangkat, dan Penyelenggaraan Pos dan Informatika Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika.

Badan Siber dan Sandi Negara. (2019). *Laporan Tahunan Honeynet Project 2019 BSSN*. Retrieved from https://cloud.bssn.go.id/s/wz4ZYiYnWjRE6cb#pdfviewer

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved from https://www.eff.org/cyberspace-independence

E.Eichensehr, K. (2015). The Cyber-Law of Nations. *The Georgetown Law Journal*, *103*(November 2014), 317–380.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *E3S Web of Conferences*, *125*(201 9), 1–5. https://doi.org/10.1051/e3sconf/201912521001

Gueham, F. (2017). *Digital Sovereignty-Steps Towards a New System of Internet Governance*. Fondation Pour L'Innovation Politique.

Hanoraga, T. (2008). Dialektika Hubungan Hukum Dan Kekuasaan. *Jurnal Sosial Humaniora*, *1*(1). https://doi.org/10.12962/j24433527.v1i1.684

Hao yeli. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Prism*, *7*(2), 109–115.

Hollis, D. B. (2012). Title : Stewardship versus Sovereignty ? International Law and the Apportionment of Cyberspace Author :, 6–14.

Irawan, J. (2018). *Pelaksanaan Yurisdiksi Universal Dalam Kedaulatan Nasional Negara-Negara (Kumpulan Ketentuan dan Praktik Kasus di Berb-*

agai Negara). Raja Grafindo Perkasa.

Isjwara, F. (1999). *Pengantar Ilmu Politik*.

Jiménez, W. G., & Lodder, A. R. (2015). Analyzing approaches to internet jurisdiction based on a model of harbors and the high seas. *International Review of Law, Computers and Technology*, *29*(2–3), 266–282. https://doi.org/10.1080/13600869.2015.1019204

Kementerian Komunikasi dan Informatika. (2009). *101 Tanya Jawab Seputar UU ITE*. Kementerian Komunikasi dan Informatika.

Kementerian Komunikasi dan Informatika. (2016). Kominfo Luncurkan Gerakan Nasional 1000 Startup Digital.

Kementerian Komunikasi dan Informatika. (2017). SIARAN PERS NO. 84/HM/KOMINFO/07/2017:Pemutusan Akses Aplikasi Telegram. Retrieved from https://www.kominfo.go.id/content/detail/10106/siaran-pers-no-84hmkominfo072017-tentang-pemutusan-akses-aplikasi-telegram/0/siaran_pers

Kementerian Komunikasi dan Informatika. (2018). Tahun 2019 Pemerintah Siapkan 20 Ribu Peserta Digital Talent Scholarship. Retrieved from https://www.kominfo.go.id/content/detail/15696/tahun-2019-pemerintah-siapkan-20-ribu-peserta-digital-talent-scholarship/0/berita_satker

Kementerian Komunikasi dan Informatika. (2019a). Indonesia Punya 5 Unicorn, Menkominfo: Ekonomi Digital Berkembang Pesat. Retrieved from https://www.kominfo.go.id/content/detail/22054/indonesia-punya-5-unicorn-menkominfo-ekonomi-digital-berkembang-pesat/0/berita_satker

Kementerian Komunikasi dan Informatika. (2019b). Proyek Palapa Ring, Satukan Indonesia Melalui Tol Langit. Retrieved from https://www.kominfo.go.id/content/detail/15978/proyek-palapa-ring-satukan-indonesia-melalui-tol-langit/0/artikel

Kementerian Komunikasi dan Informatika. (2019c). UMKM Go Online Ajak Pedagang Pasar Tradisional Go Digital. Retrieved from https://www.kominfo.go.id/content/detail/16740/umkm-go-online-ajak-pedagang-pasar-tradisional-go-digital/0/berita_satker

Kementrian Komunikasi dan Informatika. (2013). TRUST+POSITIFl. Retrieved from https://kominfo.go.id/content/detail/3322/trustpositif/0/e_business#:~:text=Sistem TRUST%2BPositif menerapkan mekanisme,profiling penggunaan internet di Indonesia.

Kementrian Komunikasi dan Informatika. (2018a). *Laporan Kinerja Kementrian Komunikasi dan Informatika 2017*.

Kementrian Komunikasi dan Informatika. (2018b). Mesin Pengais Konten Negatif Difungsikan, Tim "Trust Positif" Kominfo Dilebur. Retrieved from https://www.kominfo.go.id/content/detail/12275/mesin-pengais-konten-negatif-difungsikan-tim-trust-positif-kominfo-dilebur/0/sorotan_media

Kusumawardhana, I., & Zulkarnain. (2016). Globalisation and Strategy:Negara, Teritori dan Kedaulatan di Era Globalisasi. *Jurnal Ilmu Dan Budaya*, *40*(54), 6139–6160. Retrieved from http://journal.unas.ac.id/ilmu-budaya/article/view/363

Kusumohamidjojo Budiono. (2016). *Teori Hukum-Dilema antara Hukum dan Kekuasaan* (1st ed.). Bandung: Penerbit Yrama Widya.

Lawrence, L. (2006). *Code Version 2.0*. Basic Books.

Masyarakat Telematika Indonesia. (2015). *Kedaulatan Cyber NKRI di Era Dunia yang Serba Terhubung (globally-networked)*. Retrieved from https://mastel.id/kedaulatan-cyber-nkri-di-era-dunia-yang-serba-terhubung-globally-networked/

Medistiara, Y. (n.d.). Selama 2017 Polri tangani 3325 kasus ujaran kebencian. Retrieved from https://news.detik.com/berita/d-3790973/selama-2017-polri-tangani-3325-kasus-ujaran-kebencian

Nugraha, Y., Kautsarina, & Sastrosubroto, A. S. (2015). Towards data sovereignty in cyberspace. *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015*, (2), 465–471. https://doi.org/10.1109/ICoICT.2015.7231469

Obar, J. ., & Clement, A. (2013). Internet Surveillance and Boomerang Routing :A Call for Canadian Network Sovereignty. In *Technology & Emerging Media Track-Annual Conference of the Canadian Communication Associatin*. Retrieved from http://www.tem.fl.ulaval.ca/fr/victoriaP2013/

Proksch, W., & Schweighofer, E. (2011). Internet Governance and Territoriality Nationalisation of Cyberspace. *16th BILETA Annual Conference*, (November), 8.

Purna Cita Nugraha. (2013). Konsepsi Kedaulatan Negara dalam Boarderless Space. *Opini Juris*, *13*(Mei-Agustus).

Ridwan, H. (2011). *Hukum Administrasi Negara*. Jakarta: Raja Grafindo Perkasa.

Riyanto, S. (2012). Kedaulatan Negara Dalam Kerangka Hukum Internasional Kontemporer. *Yustisia Jurnal Hukum*, *1*(3), 5–14. https://doi.org/10.20961/yustisia.v1i3.10074

Rokhim, A. (2013). Kewenangan Pemerintah Dalam Konteks Negara Kesejahteraan (Welfare State). *Dinamika Hukum*, *XIX*(36).

Sa'diyah, N. K. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168–187.

Scerri, S. (2016). *Industrial Data Space-Digital Sovereignty Over Data*.

Schia, N. N., & Gjesvik, L. (2017). *China ' s cyber sovereignty*. https://doi.org/10.13140/RG.2.2.30512.15360

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw- Tinjauan Aspek Hukum Pidana*. Tatanusa.

Wahyudi, D., & Sumigar Bernhard Ruben Fritz, S. B. L. (2016). *Protection of personal data in Indonesia*. Jakarta. Retrieved from http://weekly.cnbnews.com/news/article.html?no=124000