Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)

Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective (Case Study of Personal Data Protection)

M. Prakoso Aji

Universitas Pembangunan Nasional "Veteran" Jakarta
Email: prakosoaji@upnvj.ac.id

Riwayat Artikel

Diterima: 19 Agustus 2022
Direvisi: 3 Oktober 2022
Disetujui: 7 Oktober 2022

doi: 10.22212/jp.v13i2.3299

Abstract

Cyber security system and data sovereignty is the foundation in realizing the protection of personal data. Technological developments place data into a very valuable commodity. In the aspect of political economy, data sovereignty of a country is faced with the position of the state with the private sector in a global context. The main role of the state is to produce cyber data protection and cyber security regulations. Guaranteed protection of personal data is a citizen's right that requires the capacity and capability of citizens. A state centered approach is often used in cyber security development. However, without a people centered approach, it will be difficult to realize protection and protection for citizens regarding their personal data which is very valuable. For this reason, this research will look at how the capacity and capability development of citizens is needed in the development of cyber security and data sovereignty related to the protection of personal data in Indonesia. The author chose qualitative research methods to facilitate the collection of data obtained through books, journal articles, online media, and other sources. The results of the study indicate that the dominance of the state-centered approach in cybersecurity development has not realized national data sovereignty, as well as the protection of the protection of the personal data of each citizen. Building the capacity and capability of citizens is very necessary to protect their personal data in cyberspace.

Keywords: *Cyber Security; Data Sovereignty; Personal Data Protection; Capability.*

Abstrak

Sistem keamanan siber dan kedaulatan data merupakan pondasi dalam mewujudkan perlindungan data pribadi. Perkembangan teknologi menempatkan data menjadi sesuatu komoditi yang sangat bernilai. Dalam aspek ekonomi politik, kedaulatan data suatu negara dihadapkan pada posisi negara dengan sektor swasta dalam konteks global. Peran negara utamanya adalah untuk menghasilkan regulasi perlindungan data siber dan keamanan siber. Jaminan perlindungan data pribadi merupakan hak warga negara yang membutuhkan kapasitas dan kapabilitas warga negara. Pendekatan berbasis state centered seringkali digunakan dalam pembangunan keamanan siber. Akan tetapi, tanpa pendekatan yang bersifat people centered akan sulit untuk mewujudkan perlindungan dan proteksi bagi warga negara terkait data pribadinya yang sangat bernilai. Untuk itu, penelitian ini akan melihat bagaimana pembangunan kapasitas dan kapabilitas warga negara diperlukan dalam pembangunan keamanan siber dan kedaulatan data terkait perlindungan data pribadi di Indonesia. Penulis memilih metode penelitian kualitatif untuk mempermudah pengumpulan data yang didapatkan lewat buku, artikel jurnal, media daring, dan sumber-sumber lainnya. Hasil penelitian menunjukkan bahwa dominasi pendekatan negara yang bersifat state centered dalam pembangunan keamanan siber belum mewujudkan kedaulatan data secara nasional, juga proteksi perlindungan data pribadi masing-masing warga negara. Pembangunan kapasitas dan kapabilitas warga negara sangat diperlukan untuk melindungi data-data pribadinya di ruang siber.

Kata Kunci: Keamanan Siber; Kedaulatan Data; Perlindungan Data Pribadi; Kapabilitas

Pendahuluan

Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak), terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber dapat digunakan sebagai sarana melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen. Dengan demikian, keamanan siber adalah semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan pada ketersediaan (*availability*), integritas (*integrity*), dan kerahasiaan (*confidentiality*) dari sebuah informasi.[1] Kerahasiaan data merujuk pada akses yang disetujui terhadap sebuah data, yang berarti hanya pihak yang memiliki akses saja yang dapat membukanya. Usaha untuk mendapatkan akses dengan cara mencuri informasi diartikan sebagai tindakan membahayakan kerahasiaan data.[2]

Selanjutnya, dalam upaya perlindungan terhadap data pribadi Menurut Privacy International dalam Prabowo, Wibawa, Azmi (2020) dikenal istilah perlindungan data (*data protection*). Definisi perlindungan data adalah sebuah aturan hukum yang bertujuan untuk memberikan perlindungan terhadap data pribadi yang dimiliki oleh seseorang. Bagi masyarakat modern, melindungi data dari penyalahgunaan adalah sangat penting. Itu sebabnya diperlukan hukum perlindungan data yang mengatur perusahaan dan pemerintah karena dua entitas ini memiliki peran yang signifikan untuk mencegah adanya penyelewengan oleh oknum yang tidak bisa dipertanggung jawabkan tindakannya. Jika tidak ada aturan hukum, banyak pihak akan dimudahkan dalam upayanya melakukan eksploitasi data.[3] Globalisasi berjalan dengan sangat cepat dalam berbagai hal, termasuk pada aspek teknologi informasi yang didalamnya terkait dengan keamanan siber dan kedaulatan data. Perkembangan media sosial yang begitu masif sudah tidak dapat dipisahkan dari perilaku keseharian setiap warga negara. Dalam setiap aplikasi baik media sosial maupun aplikasi lainnya di ruang siber mengandung begitu banyak data yang harusnya terjamin keamanannya. Apabila hal ini disalahgunakan dapat menguntungkan kelompok tertentu dan merugikan sebagian kelompok lainnya.

Perlindungan data pribadi yang dominan mengandalkan konteks keamanan yang diberikan oleh negara terhadap warga negara, belum melihat konteks kapabilitas dari warga negaranya untuk melindungi data pribadinya di ruang siber. Pengembangan kapasitas dan kapabilitas individu merupakan indikator sesungguhnya dari konsep kapabilitas yang dijelaskan oleh Amartya Sen. Pendekatan berbasis negara dalam ekonomi politik dalam konteks perlindungan terhadap data pribadi lebih dibutuhkan dalam konteks kedaulatan data antar negara, dan antar negara dengan perusahan-perusahaan kapitalis besar, di mana dalam konteks hukum kedaulatan data apabila di dalam wilayah suatu negara tidak dibangun pusat data dari perusahaan pemilik data maka negara tersebut memiliki kelemahan dalam menegakkan kedaulatannya. Oleh karena itu kapasitas dan kapabilitas warga negara dalam melindungi data-data pribadinya menjadi sangat penting agar negara tidak menjadi pihak yang dominan dalam melindungi sekaligus "mengawasi" ruang siber.

Data sebagai tenaga kerja (*data as labor*) adalah sebuah konsep yang mendudukan

1 Eric Fischer, "Cybersecurity Issues and Challenges: In Brief", *Congressional Research Service Report*, 12 Agustus 2016: 1-3.

2 Nikola Schmidt, *Cyber Security*, dalam *Introduction to Security Studies*, ed. Robert Ondrejcsak (Bratislava: Center for European and North Atlantic Affairs, 2014), 261.

3 Wisnu Handi Prabowo, Satriya Wibawa, dan Fuad Azmi, "Perlindungan Data Personal Siber di Indonesia," *Padjadjaran Journal of International Relations* 1, no. 3 (Januari 2020): 227.

data yang didapat dari perilaku pengguna internet sebagai hak miliknya sendiri. Alhasil, konsep ini jika dimanfaatkan dengan baik harusnya dapat memberikan keuntungan bagi pengguna internet itu sendiri. Perspektif *data as labor* beranggapan bahwa data itu seyogyanya dikembalikan kepada pengguna (individu) masing-masing, tanpa melihat dari apa dan bagaimana pemanfaatan data itu seterusnya. Di sisi lain, data sebagai modal (*data as capital*) memahami data sebagai sebuah sampah konsumsi digital yang tidak memiliki kegunaan, namun mengalami proses daur ulang oleh perusahaan platform digital untuk mendapatkan angka ekonomi yang tinggi. Praktik data sebagai modal dirasakan tidak sesuai dengan nilai-nilai demokrasi yang berusaha memperjuangkan hak buruh atas segala daya dan upaya yang sebelumnya semata-mata dimiliki majikan atau tuan tanah.[4] Dalam hal ini perspektif *data as labor* merepresentasikan pentingnya pengembangan kapabilitas warga negara dalam proses pembangunan.

Posisi Indonesia yang berada pada ranking ke-24 dari 194 negara, sesuai data dari Global Cyber Security Index tahun 2020, belum tentu dapat merefleksikan kebebasan yang sesungguhnya dalam kapabilitas warga negara Indonesia untuk melindung data-data pribadinya dan mendapatkan jaminan proteksi yang aman untuk dapat beraktifitas di ruang siber. Perlindungan data tiap warga negara wajib dilaksanakan, namun pada kenyataannya berbagai peristiwa yang belum lama terjadi seperti kebocoran data BPJS dan Kementerian Kesehatan, kebocoran data E-KTP, diretasnya situs Badan Intelijen Negara (BIN), dan sebagainya mempertanyakan peran dan kemampuan negara dalam konteks ini. RUU Perlindungan Data Pribadi (RUU PDP) dan RUU Keamanan dan Ketahanan Siber (RUU KKS) juga tidak kunjung disahkan oleh pemerintah.

Mosco menjelaskan dua perspektif untuk memandang dunia digital. Perspektif pertama menunjukkan bahwa ranah digital adalah ruang publik yang bersifat demokratis-deliberatif. Demokrasi digital dan kebebasan internet menjadi jargon yang terkait dengan bidang tersebut. Perspektif kedua memahami ruang digital sebagai obyek manajemen dan pengendalian bagi perusahaan-perusahaan digital global. Kekuatan pasar dimana adanya matra komodifikasi adalah faktor utama yang menentukan keputusan mengenai proses fasilitasi, produksi, pengelolaan, dan pemanfaatan informasi dari internet. Seluruh hal itu dengan oligopolistis dikendalikan oleh beberapa perusahaan teknologi digital yang memiliki jaringan transnasional.[5]

Internet, dimana menjadi komponen dari suatu *cyberspace*, telah termasuk dalam komponen integral perkembangan teknologi informasi global. Muatan-muatan informasi berkembang luas dengan pesat dengan menghasilkan metode-metode baru yang dikembangkan untuk meneruskan informasi-informasi baru tersebut. *Cyberspace* sebelumnya dipahami sebagai sebuah konteks ruang yang netral sebagai perwujudan dari inovasi dalam perkembangan teknologi global, namun saat ini tidak lagi terbebas dari berbagai kepentingan, seperti politik, ekonomi, dan sebagainya. Dalam hal ini, *cyberspace* bertransformasi sebagai ruang baru yang penuh dengan kepentingan, bahkan terkadang menjadi wadah berseterunya persaingan politik, ekonomi, dan aspek-aspek lainnya.[6] Kemudian, menurut Arifin dalam Indrawan, Efriza, dan Ilmar, digitalisasi merupakan komponen dari perkembangan teknologi informasi, yang melahirkan apa

4 Agus Sudibyo, *Jagat Digital: Pembebasan dan Penguasaan* (Jakarta: KPG, 2019), 6-7.

5 Sudibyo, *Jagat Digital*, 23-24.

6 Jerry Indrawan, "Cyberpolitics sebagai Perspektif Baru Memahami Politik di Era Siber," *Jurnal Politica* 10, no. 1 (Mei 2019): 7-8.

yang dikenal dengan internet (*international connection networking*). Konsep internet juga dipahami sebagai suatu *international network* yang menghubungkan satu dengan lainnya. Terkadang sering dikenal dengan globalisasi yang dimaknai lintas negara. Globalisasi menempatkan internet sebagai suatu komponen yang sangat penting dari perkembangan teknologi informasi global.[7]

Selanjutnya, perlindungan data pribadi masing-masing warga negara merupakan hal utama sebagai hasil dari pembangunan keamanan siber dan kemampuan kedaulatan data yang dimiliki oleh suatu negara, termasuk Indonesia. Esensi utamanya adalah hak masing-masing warga negara untuk memiliki kapabilitas dalam melindungi data-data pribadinya dan mendapatkan jaminan proteksi dari negara agar dapat "aman" dan "bebas" di ruang siber. Pembangunan pada sektor ini seharusnya juga melihat kapabilitas masyarakat untuk bisa mendapatkan perlindungan di ruang siber. Termasuk jaminan proteksi juga penting sesuai dengan konsep kebebasan Amartya Sen. Konsepsi kebebasan disini merujuk kepada "*capability approach*".

Dalam konteks ekonomi politik, pendekatan yang memiliki basis pada negara mempunyai kepentingan-kepentingan yang tidak dapat dikurangi dan berubah menjadi kepentingan-kepentingan pribadi. Pengertian otonomi negara (*state autonomy*) menunjuk pada tindakan negara untuk menjelaskan dan melakukan program dan kegiatan yang tidak berdasarkan kepentingan pribadi. Dengan demikian, pendekatan yang memusatkan kajiannya pada negara dalam konteks ekonomi politik melihat sebuah teritori politik adalah teritori negara juga atau melihat dari perspektif bahwa program negara dan ekonomi adalah program yang terkait dengan kepentingan pribadi banyak orang juga.[8]

Dalam konteks pembangunan sistem keamanan siber dan kedaulatan data, khususnya terhadap perlindungan data pribadi di Indonesia dapat dianalisis menggunakan pendekatan berbasis negara dan pendekatan kapabilitas warga negara dalam perspektif ekonomi politik terkait konteks perlindungan terhadap data pribadi di Indonesia. Akan tetapi, berdasarkan kedua pendekatan tersebut manakah yang lebih sesuai dengan konsepsi pembangunan yang sesungguhnya bagi warga negara? Dalam konteks ekonomi politik pendekatan manakah yang lebih berpihak kepada warga negara dalam konteks perlindungan data pribadi? Tulisan ini akan menjelaskan perlunya pendekatan "kapabilitas" warga negara dalam melindungi data pribadinya di ruang siber. Pembangunan keamanan siber dan kedaulatan data yang hanya bertumpu kepada negara dari aspek ekonomi politik berpotensi dapat merugikan warga negara karena berpotensi tidak memiliki kedaulatan terhadap data-data pribadinya.

Metode Penelitian

Penelitian ini menggunakan bentuk analisis deskriptif dengan metodologi kualitatif guna menjelaskan sesuatu secara intuitif dan sistematis. Penelitian ini bersifat kualitatif, dimana peneliti kualitatif berusaha mencari arti, pemahaman, definisi tentang suatu fenomena, kejadian melalui keterlibatan langsung maupun tidak langsung dalam obyek yang diteliti. Penelitian kualitatif adalah cara yang memfokuskan untuk mendapatkan makna, definisi, konsep, karakteristik, dan sebagainya termasuk deskripsi mengenai fenomena tertentu yang memiliki sifat alami dan menyeluruh yang disajikan secara narratif. Penelitian kualitatif merupakan mekanisme pencarian dan pengumpulan, termasuk analisis dan interpretasi secara komprehensif

7 Jerry Indrawan, Efriza, dan Anwar Ilmar, "Kehadiran Media Baru (New Media) dalam Proses Komunikasi Politik," *Medium Jurnal Ilmiah Fakultas Ilmu Komunikasi Universitas Islam Riau* 8, no. 1 (Juni 2020): 2.

8 James A Caporaso, David P Levine, *Teori-Teori Ekonomi Politik* (Yogyakarta: Pustaka Pelajar, 2008), 447.

untuk menghasilkan pemahaman mengenai permasalahan yang menarik.[9] Penekanan analisis dekskriptif digunakan dalam penelitian ini untuk menganalisis dan memberikan pemahaman

Jenis data dalam penelitian ini yaitu primer dan sekunder. Tekhnik pengumpulan data primer diperoleh dari studi literatur melalui buku dan artikel jurnal dimana memiliki keterkaitan terhadap keamanan siber dan kedaulatan data. Di sisi lain, data sekunder dalam penelitian ini didapatkan melalui media online dan sumber-sumber lainnya, serta digunakan sebagai data pendukung yang memiliki keterkaitan terhadap masalah penelitian. Dengan penggunaan studi pustaka, peneliti akan menjabarkan dan menganalisis sesuai dengan data dan informasi yang dikumpulkan terkait penelitian ini.

Peran Negara dalam Ruang Siber

Memaknai perkembangan teknologi dalam suatu negara tidak mungkin tanpa mengkaitkannya dengan peranan negara di dalamnya. Untuk itu, perlu memaknai negara sebagai salah satu bagian dari elemen yang terdapat di dalam politik, selain kekuasaan, pengambilan keputusan, kebijakan, dan pembagian alokasi sumber daya. Representasi kekuasaan yang terdapat dalam suatu negara demokrasi dipegang oleh pemerintah berdaulat yang mendapatkan mandat dari rakyat yang memiliki pokok tujuannya, yaitu untuk meningkatkan kesejahteraan rakyat. Adanya perkembangan teknologi berdampak besar terhadap cara-cara pemerintah menjalankan roda pemerintahan, memberikan pelayanan publik, dan memberikan kepastian hukum yang lebih baik kepada rakyatnya dengan memanfaatkan segala bentuk teknologi baru dalam ruang siber.

Terkait hal tersebut perlu terlebih dahulu kita memahami konsep mengenai negara. Harold J.Laski dalam Syaiful Bakhri (2018) berpandangan bahwa negara memiliki kewenangan yang secara sah dapat memaksa individu-individu atau kelompok-kelompok yang menjadi bagiannya. Negara juga bisa disebut sebagai suatu masyarakat atau kelompok manusia yang hidup, bekerja sama, dan terintegrasi untuk mewujudkan keinginan bersama. Dalam sebuah negara, cara masyarakat hidup harus ditaati bersama dan diawasi oleh negara karena memiliki kewenangan mengikat dan dapat memaksa.[10]

Keamanan siber dapat dipahami sebagai sebuah konsep, teknologi, pedoman, kebijakan, pelatihan, praktek, jaminan, dan tindakan keamanan yang berguna untuk melindungi organisasi, aset, dan lingkungan siber pengguna. Dalam sebuah keamanan lingkungan siber terdapat perangkat yang dihubungkan dengan infrastruktur, aplikasi, komputasi, layanan, sistem telekomunikasi dan informasi yang termasuk dalam organisasi dan aset pengguna. Dengan demikian, memelihara dan memastikan aset pengguna dan organisasi aman terhadap ancaman atau resiko keamanan yang mungkin muncul di ranah siber, adalah salah satu fungsi dari keamanan siber.[11] Peran negara dan pemerintah merupakan hal yang tidak dapat dibedakan. Kita juga bisa memahami bahwa di ranah siber peran pemerintah sebagai representasi kekuasaan yang menyatakan bahwa negara hadir di dalam ruang siber untuk mengatur kehidupan warganya dalam rangka mencapai tujuan bersama untuk mensejahterakan kehidupan rakyat terbukti sangat besar.

Berkaitan dengan peran negara dalam ruang siber dalam konteks nasional, maka perlu disusun suatu regulasi yang jelas dan

9 A Muri Yusuf, *Metode Penelitian: Kuantitatif, Kualitatif & Penelitian Gabungan* (Jakarta: Kencana, 2017), 328-330.

10 Syaiful Bakhri, *Ilmu Negara: Dalam Pergumulan Filsafat, Sejarah dan Negara Hukum* (Depok: Rajawali Pers, 2018), 38.

11 Handrini Ardiyanti, "Cyber Security dan Tantangan Pengembangannya di Indonesia," *Jurnal Politica* 5, no 1 (Juni 2014): 98.

detail sebagai pedoman bagi warga negara dalam beraktifitas di dalam ruang siber, juga untuk menjamin kedaulatan negara maupun warga negaranya dari data-data yang berkaitan dengan dirinya. Untuk mengawasi aktifitas warga negara dalam semangat yang demokratis, kritis, tetapi tetap tidak kebablasan, diperlukan regulasi hukum yang dikeluarkan oleh negara yang berfungsi sebagai rambu-rambu.

Terkait perlunya disusun dasar hukum yang jelas sebagai pedoman aktivitas warga di ruang siber, menurut Boele-Woelki dalam Nudirman Munir (2017), dibutuhkan peran dan keterlibatan pemerintah secara langsung untuk membuat regulasi di ruang siber, utamanya untuk menyelesaikan masalah (hukum atau non-hukum) yang bisa timbul. Tom Maddox dalam Munir sejalan dengan Boele-Woelki, perbedaannya hanya pada fungsi pengendalian saja.[12] Kelemahan dunia siber di Indonesia disebabkan karena minimnya pengaturan terkait siber yang berakibat pada timbulnya kerancuan di tengah anggota masyarakat. Dunia siber yang melewati batas-batas negara, batas wilayah kepemilikan, hingga batasan pribadi yang berakibat timbulnya konflik juga sengketa yang terjadi di tengah anggota masyarakat.[13]

Dalam konteks Indonesia, pada tahun 2017 Presiden Jokowi membentuk Badan Siber dan Sandi Negara atau biasa disingkat BSSN. Pembentukan BSSN yang merepresentasikan hadirnya negara dalam pengelolaan ruang siber nasional memilki peranan yang penting untuk mengoptimalkan koordinasi juga kerjasama lembaga-lembaga lainnya selaku stakeholder dalam ranah siber di Indonesia. Stakeholder lainnya terkait ruang siber nasional yaitu: TNI/ Kementerian Pertahanan (terkait pertahanan siber), Polri (terkait kejahatan siber), Kementerian Luar Negeri (diplomasi siber), dan kementerian/ lembaga lainnya yang terkait dengan tupoksi di bidang siber. Dalam perjalanannya, BSSN sebetulnya telah menjalankan pembinaan terkait *cyber security community*. Terkait fungsi dari proteksi ini ada pada Deputi II bidang proteksi yang memiliki tugas dalam bidang tata kelola keamanan informasi.[14] Hal ini tidak terlepas dari sebagian besar unit kerja BSSN sebelumnya berasal dari Lembaga sandi Negara (Lemsaneg). Lemsaneg sudah didirikan sejak lama, bahkan sejak era Soekarno dengan bentuk jawatan sandi. Tupoksi Lemsaneg terkait dengan persandian yang memiliki fokus pada keamanan informasi. Dalam hal ini fungsi keamanan informasi memiliki kedekatan substansial dengan keamanan siber yang menjadi tupoksi dari BSSN saat ini.

Menurut mantan Kepala BSSN, Djoko Setiadi, BSSN mampu mendeteksi ancaman siber yang terjadi sepanjang 2018. Dengan kemampuan deteksi ini diharapkan agar semua pihak bisa memahami pergeseran perilaku serangan siber. Terkait kemampuan tersebut, BSSN telah mendeteksi jumlah serangan sepanjang Januari hingga Oktober 2018, sebanyak 207.9 juta serangan. Serangan paling banyak adalah melalui virus *trojan*. Selain itu, sebanyak 36 juta aktivitas *malware* juga menyerang situs-situs penting di Indonesia.[15] Kasus peretasan hacker di Indonesia belum lama ini juga terjadi yang menghadirkan nama "Bjorka" menjadi perhatian publik. Selain kasus "Bjorka" terdapat beberapa kasus-kasus lain yang meresahkan publik khususnya terkait permasalahan perlindungan data pribadi. Pada Bulan Mei Tahun 2021, BPJS Kesehatan juga mengalami peretasan yang menyebabkan kebocoran data sejumlah besar

12 Nudirman Munir, *Pengantar Hukum Siber di Indonesia* (Depok: Rajawali Pers, 2017), 30.

13 Munir, *Pengantar Hukum Siber*, 27.

14 Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara," *Jurnal Politica* 10, no. 2 (November 2019): 122-123.

15 Amal Nur Ngazis, "Badan Siber: 36 Juta Malware Serang Situs Penting Indonesia," *Viva*, 12 Desember 2018, diakses 12 Desember 2021, https://www.viva.co.id/digital/ digilife/1102720-badan-siber-36-juta-malware-serang-situs-penting-indonesia

Warga Negara Indonesia. Termasuk juga beberapa kementerian/lembaga yang diretas oleh hacker yang menyebabkan kebocoran data, terutama data-data pribadi pegawai instansi tersebut, dan data-data lainnya.[16] Sedangkan pada Tahun 2022, menurut data BSSN di Indonesia telah terjadi lebih dari 700 juta serangan siber. Serangan siber ini didominasi oleh *malware* maupun *ransomware* yang memiliki motif menginginkan sejumlah tebusan.[17] Sedangkan sebelumnya pada Tahun 2021, data BSSN menyampaikan bahwa di Indonesia terjadi 1,6 Miliar serangan siber yang didominasi kategori *malware*.[18]

Dalam hal ini, jumlah data serangan siber di Indonesia dapat merepresentasikan bahwa keamanan siber merupakan hal yang fundamental dalam kehidupan berbangsa dan bernegara. Bangsa yang berdaulat merupakan bangsa yang juga memiliki kedaulatan terhadap data-data pribadi yang dimiliki oleh warga negaranya dari serangan-serangan siber. Oleh karena itu, sudah sepatutnya warga negara Indonesia memiliki pemahaman dan kemampuan terkait urgensi dari melindungi dan menjaga data pribadi yang dimilikinya. Kemampuan warga ini terkait kapabilitas dari warga negara Indonesia mengenai kemampuan, kesadaran, wawasan, gagasan, dan akses yang dimiliki oleh masing-masing individu untuk melindungi data-data pribadinya.

Melindungi data personal secara umum didasari pada konsep penentuan nasib sendiri yang informatif (*informational self-determination*). Konsep ini menentukan individu untuk memilih data yang akan dibagi, berdasarkan kepentingan apa, dan untuk siapa data itu akan diberikan. Pengguna jadi bisa menentukan privasinya sendiri ketika menggunakan platform-platform teknologi yang bersifat layanan publik, seperti Google misalnya. Konsep ini percaya bahwa melindungi privasi individu harus dilakukan melalui peraturan yang jelas dan tegas oleh negara, sehingga juga berdampak pada kegiatan ekonomi yang dihasilkannya. Dengan demikian, penyedia layanan teknologi, yang adalah para perusahaan-perusahaan besar ini, dalam kontek persaingan bisnis, harus tetap menghormati privasi konsumennya.[19]

Menurut Schünemann & Baumann dalam Prabowo, dkk (2020), penentuan nasib sendiri ini harus sejalan dengan keahlian untuk memahami proses transfer, pemrosesan data, dan kapasitas penyimpanan untuk menentukan pengesahan yang diminta. Ditambah lagi, pengesahan itu juga tidak boleh diintervensi pihak luar. Bagi perusahaan-perusahaan besar, konsep ini akan menjadi masalah bagi layanan sosialnya, seperti Google atau Facebook misalnya. Masalah muncul karena kekuatan jaringan perusahaan-perusahaan teknologi besar itu bersifat monopolistik. Kondisi demikian membuat privasi individu pengguna menjadi sulit saat proses digitalisasi semakin berkembang.[20]

Menurut pendapat penulis, pembangunan sektor keamanan siber merupakan pondasi awal menyusun kemampuan kedaulatan negara terkait data dan informasi di ruang

16 Mirsya Anandari Utami, "5 Kasus Serangan Siber yang Pernah Terjadi di Indonesia Sebelumnya," *Okezone*, 21 September 2022, diakses 28 September 2022, https://techno.okezone.com/read/2022/09/21/54/2672211/5-kasus-serangan-siber-yang-pernah-terjadi-di-indonesia-sebelumnya

17 CNN Indonesia, "RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan," *CNN Indonesia*, 1 Juli 2022, diakses 28 September 2022, https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan#:~:text=Jakarta%2C%20CNN%20Indonesia%20%2D%2D,malware%20dengan%20modus%20meminta%20tebusan.

18 Witri Gustiani, "Terjadi 1,6 Miliar Serangan Siber Sepanjang 2021, Bagaimana dengan 2022 dan Kemunculan Bjorka?" *Pikiran Rakyat*, 27 September 2022, diakses 28 September 2022, https://www.pikiran-rakyat.com/nasional/pr-015583077/terjadi-16-miliar-serangan-siber-sepanjang-2021-bagaimana-dengan-2022-dan-kemunculan-bjorka

19 Prabowo, Wibawa, Azmi, "Perlindungan Data Personal Siber di Indonesia," 229.

20 Prabowo, Wibawa, Azmi, "Perlindungan Data Personal Siber di Indonesia," 229.

siber. Akan tetapi apabila lebih menekankan pada kemampuan negara maka cenderung melekatkan pemahaman konsep *data as capital*. Pengembangan kapabilitas warga negara terkait keamanan data dan informasi perlu lebih ditekankan sehingga data dapat dianggap sesuai konsep *data as labor*.

Penulis saat ini menyakini bahwa konteks perlindungan data yang *self-determination* belum dapat menyentuh pembangunan kapabilitas dari warga negara itu sendiri. Bahkan konteks *self-determination* ini sangat memerlukan regulasi yang mewadahinya. Regulasi ini merupakan produk dari negara yang memiliki tujuan untuk menciptakan keamanan dan ketertiban, juga mewujudkan kesejahteraan masyarakat. Saat ini di Indonesia Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi belum lama telah disahkan menjadi undang-undang. Regulasi ini diharapkan dapat menjadi harapan baru bagi permasalahan perlindungan data di Indonesia. Namun, terkait Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber belum disahkan hingga saat ini.

Hal ini menimbulkan kekosongan regulasi dalam pengembangan ruang siber nasional yang dihadapkan pada konteks pembangunan keamanan siber dan permasalahan kedaulatan data. Menurut pendapat penulis, solusinya adalah pembangunan kapabilitas warga negara terkait hal ini. Pembangunan tersebut merupakan kunci utama indikator pembangunan yang sesungguhnya. Sistem keamanan siber dan kedaulatan data di Indonesia bertumpu pada aturan yang dibuat negara. Apalagi dalam perspektif ekonomi politik, di mana perusahaan-perusahaan besar dunia yang menguasai data bisa masuk dan "mengacak-acak" kedaulatan negara kita demi keuntungan finansial.

Kedaulatan Data dalam Perspektif Ekonomi Politik

Perkembangan digitalisasi menurut Schiller dalam Sudibyo (2019), berkontribusi pada terciptanya sebuah ranah siber yang sulit tersentuh aturan, baik aturan nasional, apalagi internasional. Hukum dalam konteks pengaturan media pun sangat sulit menyentuh dunia digital ini, apalagi hukum persaingan usaha misalnya, atau bahkan hukum pajak. Ketidakmampuan mengaplikasikan aturan hukum ini menghambat proses pengawasan dan pengaturan perusahaan-perusahaan digital besar, seperti Google dan Facebook tadi misalnya. Dampak yang terjadi adalah, menghindari pajak, alih daya digital yang menyebabkan pengangguran, mundurnya media-media cetak, termasuk ketimpangan ekonomi karena praktik kapitalisme. Dalam konteks yang terkait, beberapa pakar lintas disiplin yaitu Vincent Moso, Bill Kovach, Robert McChesney, dan Soshana Zuboff dalam Sudibyo (2019) meletakkan perkembangan teknologi secara luas, khususnya dalam hal hubungan kekuasaan. Internet dan platform-platformnya, seperti media sosial, *e-commerce*, atau *search engine* tidak saja pada fenomena teknologi informasi atau ilmu matematika terapan, tetapi juga fenomena ekonomi politik yang dapat merubah masyarakat juga tatanan sosial. Internet pada saatnya dapat menggambarkan kekuatan ekonomi politik antar negara yang mampu menentukan nasib suatu negara yang terjadi pada Pemilihan Presiden Amerika Serikat pada tahun 2016.[21]

Melalui perspektif globalisasi, dapat dipahami bahwa penyebaran nilai-nilai budaya juga merupakan bagian untuk mempertahankan pengaruh negara maju kepada negara berkembang. Dalam aktivitas masyarakat dunia siber kondisi ini dapat dipahami sebagai suatu *power* dalam dunia yang tak kasat mata. Hal ini dalam konteks internasional akan berimplikasi pada sektor pertahanan dan keamanan di ruang siber, di mana eksistensinya berada pada suatu

21 Sudibyo, *Jagat Digital*, 17.

dunia yang tak kasat mata, saling terhubung (*connectivity*), tanpa batas (*borderless*), dan dengan aksesibilitas yang sangat tinggi (*accessible*). Terjadi persaingan antar-negara di dunia dalam penguasaan teknologi, yang dapat menempatkan negara yang memiliki teknologi lebih canggih untuk memiliki kedudukan dan pengaruh yang lebih dibandingkan negara lainnya. Hal ini juga terjadi dalam penguasaan teknologi dalam ruang siber. Suatu negara yang memiliki teknologi di bidang siber yang lebih canggih akan memiliki daya tawar yang lebih tinggi dibandingkan negara lainnya. Dalam situasi tertentu aspek politik di ruang siber juga sangat berpengaruh dalam konteks kedaulatan.

Masalah-masalah yang dibahas dalam politik siber terkait dengan kekuasaan dan kepentingan nasional, yang menjadi alasan mengapa politik siber berhubungan erat dengan kedaulatan negara. Dalam konteks kekuasaan, kita bisa melihat pemilu sebagai sebuah kontestasi politik yang melibatkan banyak aktor, seperti masyarakat, penyelenggara, dan tentunya kontestan pemilu itu sendiri, di mana kesemuanya berpartisipasi di ranah siber. Contoh lainnya, birokrasi pemerintah menjadi sangat ketinggalan zaman karena masif dan cepatnya dinamika pergerakan dimensional politik siber tersebut.[22]

Keterkaitan ruang siber dengan politik siber sangat erat, yang memang bisa masuk kategori *low politics*. Berbeda dengan isu *high politics*, yang mana isu-isunya dapat berupa kepentingan nasional sebuah negara, keamanan nasional sebuah negara, keputusan strategis yang harus diambil sebuah negara, nasionalisme, konflik, atau bahkan perang, isu *low politics* menggambarkan sebuah definisi yang menampilkan latar belakang negara dalam proses pengambilan keputusannya.[23]

Dengan demikian, menurut penulis dinamika yang terjadi saat ini, yang berhubungan dengan politik siber, maupun ruang siber akan menggantikan isu *high politics*, sehingga isu-isu *low politics* tidak akan ada di bawah permukaan lagi seperti dahulu. Politik siber lama-kelamaan akan menjadi bagian integral dari isu-isu *high politics*, salah satunya karena diskursus yang terjadi di ruang siber sudah melampai terminologi *low politics* lagi. Negara yang secara konstan merasa terancam oleh pihak-pihak lain, sudah harus menganggap ruang siber sebagai ancaman bagi kedaulatan mereka.

Kondisi di atas memiliki dampak pada kepentingan nasional (*national interest*) yang dimiliki oleh suatu negara yang tujuannya untuk menjaga keamanan dan mensejahterakan rakyatnya, di mana dalam ruang lingkup global dapat mempengaruhi masa depan dari jutaan warga negara lainnya, karena bentuk hubungan yang tercipta antar-negara tersebut menjadi tidak sejajar. Dengan demikian, sudah menjadi tugas pemerintah masing-masing dalam suatu negara untuk memiliki kemampuan penguasaan teknologi dalam ruang siber yang mumpuni sebagai representasi kekuatan pertahanan dan keamanan negara tersebut dalam kancah global. Kondisi ini akan berimplikasi kepada banyak aspek bagi kehidupan rakyatnya, baik secara ekonomi politik, komunikasi politik internasional, sosial budaya, serta aspek-aspek lainnya yang terkait.

Dalam konteks ekonomi politik internasional, keamanan informasi dan intelijen siber (*cyber intelligence*) merupakan dua hal penting karena bagian dari kemampuan suatu negara untuk menjaga kedaulatannya dalam aspek informasi, terutama hal-hal yang dapat diklasifikasikan sebagai rahasia negara. Keamanan informasi dalam suatu negara juga tidak saja menyangkut hal-hal yang dapat

22 Suwandi Sumartias (ed), *Keamanan Siber dan Pembangunan Demokrasi di Indonesia* (Jakarta: Pusat Penelitian Badan Keahlian DPR RI dan Intrans Publishing, 2018), 7.

23 M. Prakoso Aji dan Jerry Indrawan, *Cyberpolitics: Perspektif Baru Memahami Politik Era Siber* (Depok: Rajawali Pers, 2019), 11.

diklasifikasikan sebagai rahasia negara, tetapi juga hal-hal yang menyangkut hajat hidup rakyatnya di semua dimensi dan bidang kehidupan. Sedangkan kemampuan *cyber intelligence* yang mumpuni sangat diperlukan suatu negara untuk mempertahankan kedudukannya di dunia internasional, baik dalam hubungan internasional, maupun masalah-masalah keamanan dan pertahanan.

Kedaulatan data suatu negara sangat dipengaruhi oleh keberadaan pusat data yang ada di wilayah teritorialnya atau tidak. Apabila perusahaan-perusahaan besar seperti Facebook, Twitter, WhatsApp, Google tidak membangun pusat datanya di suatu negara, maka negara tersebut tidak dapat memiliki kekuatan hukum untuk dapat menjamin data-datanya aman dan tidak disalahgunakan. Hal inilah yang menjadi kendala utama dalam konteks kedaulatan data. Sebagian besar negara-negara berkembang tidak memiliki "*power*" karena perusahaan-perusahaan besar tersebut tidak membangun pusat datanya di wilayah mereka, walaupun masyarakat di negara-negara berkembang merupakan pangsa besar bagi perusahaan-perusahaan teknologi tersebut. Hal ini juga yang terjadi di Indonesia. Perusahaan-perusahaan besar seperti Facebook, WhatsApp, Google, Twitter, dan lain-lain belum seluruhnya membangun pusat datanya di Indonesia. Hal ini akan sangat menyulitkan Indonesia apabila suatu saat dihadapkan pada kondisi "krisis" kedaulatan data.

Pada bulan April 2016, muncul regulasi yang melembagakan perlindungan data orang-orang yang menggunakan internet sebagai hak milik orang-orang tersebut. GDPR General Data Protection Regulation atau GDPR merupakan sebuah aturan setingkat undang-undang, yang dilegalkan oleh Parlemen Uni Eropa, yang melindungi warga Uni Eropa dari penyalahgunaan dan penyelewengan, maupun kejahatan siber, terkait perlindungan data pribadi mereka. Pihak-pihak eksternal, seperti perusahaan-perusahaan penyedia layanan digital yang memberikan layanan media sosial, surat elektronik, mesin pencari, dan perdagangan elektronik ditengarai kerap kali melakukan penyalahgunaan data pribadi konsumen. Itu sebabnya GDPR menjadi regulasi yang akan diproyeksikan sebagai *role model* untuk melakukan perlindungan data pribadi di internet. Siapa pun, baik individu atau perusahaan yang mengumpulkan, menganalisis, melakukan komodifikasi, baik seluruhnya atau sebagian, data perilaku pengguna internet warga Uni Eropa, harus mematuhi ketentuan sesuai regulasi GDPR.[24] Dalam konteks Indonesia, relatif hanya UU ITE yang dapat dikaitkan dengan regulasi kedaulatan dan perlindungan data di Indonesia. Akan tetapi kandungan substansi di dalam UU ITE dirasakan belum cukup menjadi regulasi untuk mewujudkan kedaulatan data nasional. Walaupun belum lama UU Perlindungan Data Pribadi (PDP) sudah disahkan, publik masih menunggu implementasi dari regulasi ini ke depannya.

Dalam UU ITE dunia siber tidak diartikan secara definitif. Dalam UU ITE dunia siber hanya diartikan dalam penjelasan, yaitu kegiatan melalui media elektronik. Kata "kedaulatan" secara terminologi hanya terlihat dalam penjelasan Pasal 2 UU ITE yang berkaitan dengan cakupan "merugikan kepentingan Indonesia" terkait bagian berlakunya UU ITE. Dalam pasal 2 UU ITE timbul konsep kedaulatan yang ditegaskan mengenai berlakunya ketentuan pada UU ITE mengacu pada akibat dan kerugian dari tindakan yang dilakukan, tidak melihat tindakan itu apakah terjadi dalam kewenangan area hukum Indonesia atau di luar area hukum Indonesia. Kerugian tersebut merupakan kerugian yang terkait dengan kepentingan Indonesia, tidak hanya terkait perekonomian nasional, kepentingan memberikan keamanan

24 Sudibyo, *Jagat Digital*, 8-9.

data, dan kepentingan strategis lainnya, namun juga termasuk kedaulatan negara. Ancaman hukuman dapat dikenakan pada perbuatan yang dilarang pada Pasal 27 hingga Pasal 36 UU ITE yang dijalankan di luar area Indonesia terhadap sistem elektronik yang ada di Indonesia.[25]

Terkait konteks keamanan siber, menurut penulis pembentukan BSSN memberi harapan baru dan juga solusi untuk mewujudkan kedaulatan data nasional. Akan tetapi nampaknya masih banyak permasalahan yang menyebabkan lembaga ini belum mampu bekerja secara optimal. Permasalahan utama disebabkan absennya aturan, dalam hal ini belum disahkannya RUU Kemanan dan Ketahanan Siber di parlemen. Sedangkan UU Perlindungan Data Pribadi juga baru saja disahkan sehigga belum dapat diukur implementasinya. Selain itu, penulis juga berpendapat bahwa dua regulasi di bidang siber ini sebaiknya melibatkan aspirasi dari masyarakat untuk menjaga nilai-nilai demokrasi yang kita pegang teguh. Gagasan mengenai perlunya dibentuk semacam Komisioner yang mengawasi kebijakan dari UU Perlindungan Data Pribadi seyogyanya patut dipertimbangkan agar memberikan makna yang lebih demokratis dalam penerapan regulasi ini. Dengan adanya pengawasan yang melibatkan partisipasi masyarakat diharapkan konteks perlindungan data dapat lebih optimal sehingga data dapat memberikan manfaat bagi pemilik datanya sebagai suatu properti yang bernilai.

Selain itu, *job desk* BSSN sangat berkaitan dengan kementerian/lembaga (K/L) lainnya. Salah satu K/L yang paling berhubungan dengan lembaga ini tentu adalah Kementerian Komunikasi dan Informatika (Kominfo). Tugas menyelidiki kejahatan siber sudah menjadi tugas, pokok, dan fungsi unit Kejahatan Siber (*Cyber Crime*) Mabes Polri. Tugas pertahanan negara dari sisi siber (*cyber defence*) menjadi ranahnya Kementerian Pertahanan (Kemhan), yang mana saat ini sudah memiliki Pusat Operasi Siber (*Cyber Operation Center*). Penanganan penipuan perdagangan elektronik ditangani oleh Kementerian Perindustrian, Kementerian Perdagangan, dan Kominfo, diplomasi siber oleh Kementerian Luar Negeri (Kemlu), operasi intelijen siber oleh BIN, dan kejahatan keuangan dan ekonomi digital ditangani oleh PPATK dan KPK. Di sisi lain, pihak swasta juga saat ini sudah banyak yang berbisnis di bidang pengamanan untuk melindungi infrastruktur-infrastruktur kritis negara. Menjadi problematikan menarik untuk penulis bahas disini karena BSSN diatur tugas, fungsi, dan wewenangnya di dalam Peraturan Presiden (Perpres). Namun, dalam realitanya mereka harus mengoordinasikan sejumlah K/L yang dasar hukumnya adalah undang-undang. Itu sebabnya mengapa kinerja BSSN belum optimal karena kebutuhan yang ada tidak bisa dijawab selama regulasi di bidang siber belum diperbaharui.[26]

BSSN memberikan laporan kepada publik bahwa pada tahun 2019 terdapat 290 juta kasus serangan siber, meningkat 25% dari tahun sebelumnya, dan membuat negara rugi sebesar US$ 34,2 miliar. Peraturan-peraturan yang berkaitan dengan keamanan siber di Indonesia dibagi ke beberapa K/L menjadi tanggung jawab sektoral mereka. Cara ini sangat tidak efektif jika kita ingin mencegah ancaman siber ini. Solusinya adalah harus ada aturan hukum komprehensif agar semua penegak hukum dapat bergerak bersama menangani persoalan siber, bukan bergerak sendiri-sendiri mengedepankan ego sektoral.[27]

Kapabilitas dan Kebebasan Dalam Perlindungan Data Pribadi di Indonesia

25 Siti Yuniarti, Erni Herawati, "Analisis Hukum Kedaulatan Digital Indonesia," *Pandecta Jurnal Penelitian Ilmu Hukum* 15, no. 2 (Desember 2020): 159-160.

26 DPR-RI, "Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber," *DPR-RI*, diakses 12 Desember 2021, https://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf.

27 Noor Halimah Anjani, "Perlindungan Keamanan Siber di Indonesia," *CIPS Ringkasan Kebijakan* 9 (Maret 2021): 1.

Amartya Sen menjelaskan bahwa "*space*" yang tepat adalah kebebasan substantif, yaitu kapabilitas yang dimiliki individu untuk memilih dan mencapai tujuannya pada kesempatan yang sesungguhnya. Dalam hal ini tidak hanya "*primary goods*" yang dimiliki oleh masing-masing orang, tetapi juga melihat karakteristik pribadi yang dapat digunakan untuk mencapai tujuannya. Konsep "*functionings*" dapat mencerminkan berbagai hal bahkan hingga kepada hal yang sangat kompleks seperti bagaimana seseorang dapat memiliki harga diri dan ikut ambil bagian dalam kehidupan masyarakat. Kapabilitas seseorang mengacu pada kombinasi alternatif fungsi yang layak untuk dicapainya. Dengan demikian Kapabilitas adalah bentuk dari kebebasan, dalam hal ini kebebasan substantif untuk mencapai kombinasi fungsi alternatif. Fokus evaluatif dari "*capability approach*" dapat berupa realisasi dari fungsi tersebut (apa yang sebenarnya dapat dilakukan seseorang) atau pada rangkaian alternatif kemampuan yang dimilikinya (peluang sesungguhnya yang dimiliki seseorang). Berdasarkan tradisi di bidang ekonomi, nilai sesungguhnya dari serangkaian pilihan terdapat pada penggunaan terbaik yang dapat dilakukan dari pilihan-pilihan tersebut.[28]

Amartya Sen berpandangan bahwa pembangunan yang sesungguhnya seharusnya memberikan kesempatan bagi manusia untuk memutuskan pilihan dalam kehidupannya yang bernilai. Oleh karena itu, pembangunan yang berhasil dapat memberikan kesempatan bagi masyarakat untuk mengimplementasikan pilihannya secara aman dan bebas. Dalam konteks pembangunan di Indonesia, perkembangan keamanan siber dan kapabilitas warga negara dalam perlindungan data pribadi merupakan hal yang menarik untuk diteliti lebih jauh agar dapat melihat konteks pembangunan yang sesungguhnya dalam bidang teknologi informasi ini yang juga sangat terkait dengan pembangunan ekonomi di Indonesia. Perlindungan data pribadi merupakan hal yang esensial karena berkaitan dengan kedaulatan pada aspek ekonomi politik, baik dalam skala yang besar yaitu antar negara yang satu dengan lainnya, hingga hak asasi dari masing-masing warga negara itu sendiri. Di dalamnya berkaitan dengan informasi, seperti Kartu Data Penduduk (KTP), data kesehatan, rekening bank, bahkan hingga data rekam mobilitas individu yang seringkali digunakan saat ini dalam konteks penanganan pandemi.

Instrumen pertumbuhan teknologi informasi seperti: jumlah serangan siber yang terdeteksi, banyaknya *unicorn* teknologi, seperti Tokopedia, Gojek, Buka Lapak, dan sebagainya yang tumbuh di Indonesia, belum dapat menjawab makna kebebasan yang sesungguhnya bagi warna negara dalam peningkatan kesejahteraan. Bagi warga negara yang tidak memiliki pengetahuan terhadap berbagai aplikasi, teknik dan metode keamanan data, berpotensi menjadi individu yang rentan terhadap ancaman keamanan data dan informasi yang dimilikinya. Termasuk warga negara penyandang disabilitas, individu yang tinggal di wilayah yang sulit menjangkau jaringan internet akan sangat kesulitan untuk memiliki kapabilitas yang merefleksikan kebebasan dan kesejahteraan yang sesungguhnya dalam pembangunan pada sektor ini. Jaminan proteksi dari negara terhadap warganya diperlukan, namun tidak boleh mematikan ruang-ruang demokrasi di ruang siber.

Menurut Amartya Sen, pembangunan manusia (*human development*) didefinisikan sebagai sebuah metode perluasan kesempatan untuk memberikan keputusan terkait pilihan-pilihan dalam kehidupan seorang manusia. Dengan demikian, keamanan manusia (*human security*) adalah sebuah masyarakat yang secara

28 Amartya Sen, *Development as Freedom* (New York: Alfred A. Knopf, 1999), 75-76.

bebas dan aman mampu menerapkan pilihan-pilihannya, dengan tujuan untuk melestarikan dirinya sendiri agar tidak musnah di masa depan. Ada beberapa karakteristik utama menurut Sen, yaitu *interdependent*, *people centered*, dan *universal concern*.[29]

Sabina Alkire dalam Prabowo, Wibawa, Azmi (2020) berargumen bahwa konsep keamanan manusia harus menjaga inti vital dari negara dan melindunginya terhadap ancaman yang saat ini bersifat multi-dimensional. Kebutuhan jangka panjang negara dan manusia di dalamnya harus dijaga secara konsisten, termasuk hak untuk hidup, hal untuk mendapatkan pekerjaan, dan hak untuk dihargai sebagai seorang manusia. Pemahaman ini berdasarkan argumentasi praktis yang disematkan untuk mengkategorisasikan prosedur pada beberapa bentuk terkait definisi *freedom from fear* dan *freedom for want* yang sifatnya luas. Dalam hal ini,*vital core* melihat pada istilah non-teknis yang dapat didefinisikan sebagai *space of capability*, *the freedom people have to do and to be*. Seluruh pihak mendapatkan kewajiban untuk menjaganya, walaupun dengan kemampuan yang ada tidak akan mungkin dapat dilakukan dengan sempurna. Oleh karena itu, elemen *vital core* merupakan hak asasi yang mendasar. Institusi yang dapat menghasilkan keputusan yang adil sangat dibutuhkan dalam mempertimbangkan prioritas antara hak dan kapabilitas. Partisipasi dari pihak atau institusi yang haknya terancam sangatlah diperlukan.[30]

Di Indonesia, sebelum disahkannya UU Perlindungan Data Pribadi pada tanggal 20 September 2022, tidak terdapat peraturan yang menjelaskan tentang definisi "hak privasi", kecuali di Pasal 28 ayat 1 Undang-Undang 1945. Pada pasal tersebut tercantum berbagai hak yang berhubungan dengan privasi. Terkait perlindungan data, hak privasi memiliki kedekatan makna dan kaitan. Individu, sebagai seorang pengguna, harus punya metode untuk menerapkan hak privasi mereka agar terlindungi, berkaitan dengan perlindungan data pribadi mereka. Di dalam negara hukum, kewajiban perlindungan data harus jelas dimasukkan dalam undang-undang, sehingga ada langkah-langkah mitigasi terhadap gangguan atau ancaman hak privasi seseorang. Kemudian, para perusahaan-perusahaan besar yang mencoba menganggu keamanan data pribadi seseorang, dapat dimintai pertanggung jawabannya secara hukum.[31]

Pada tahun 2021 lalu telah terjadi beberapa insiden kebocoran data baik data yang ada di kementerian/lembaga, maupun data-data pribadi warga negara yang ada di lembaga pelayanan publik lainnya maupun sektor swasta. Peretas dari China dilaporkan berhasil menerobos tembok api (*firewall*) dari sekitar 10 K/L di Indonesia, di mana dalamnya termasuk milik Badan Intelijen Negara (BIN). Aksi ini ditenggarai dilakukan oleh Mustang Panda, seorang peretas China, yang sering menyasar negara-negara di Asia Tenggara, demikian menurut hasil penelitian lembaga keamanan internet The Record, Insikt Group.[32]

Terkait hal ini, masyarakat memiliki peranan penting dalam menjaga kedaulatan negara dalam ruang siber. Hal itu dapat tercermin dari tingkat kesadaran keamanan informasi masyarakat. Menurut Pratama Persada, masyarakat Indonesia belum memiliki kesadaran besar melakukan pengamanan aset-aset digitalnya. Kejadian virus r*ansomware wannacry* pada tahun 2017 lalu membuktikan bahwa hanya 33% masyarakat dan institusi swasta yang mematuhi saran Kemenkominfo

29 Prabowo, Wibawa, Azmi. "Perlindungan Data Personal Siber di Indonesia," 222.

30 Prabowo, Wibawa, Azmi, "Perlindungan Data Personal Siber di Indonesia," 223.

31 Prabowo, Wibawa, Azmi, "Perlindungan Data Personal Siber di Indonesia," 227 dan 229.

32 CNN Indonesia, "Jaringan BIN dan Kementerian Dilaporkan Dibobol Hacker China," *CNN Indonesia*, 12 September 2021, diakses 10 Desember 2021, https://www.cnnindonesia.com/nasional/20210912112723-20-693110/jaringan-bin-dan-kementerian-dilaporkan-dibobol-hacker-china.

untuk mengatur Windows *Personal Computer* (PC) dan komputer jinjing mereka. Sebanyak 67% tidak melakukan apa pun. Sebuah realitas yang menunjukkan lemahnya kesadaran untuk melakukan pengamanan data digital pada masyarakat kita. Sayangnya, rendahnya kesadaran keamanan siber juga ditunjukkan oleh para pejabat tinggi negara yang masih merasa bahwa keamanan siber di Indonesia belum menjadi ancaman serius. Kondisi ini meningkatkan kemungkinan terjadinya spionase dari negara asing atau ancaman internal dari dalam negeri sendiri, yang ingin membuat kekacauan.[33]

Oleh karena itu dalam pembangunan sistem keamanan siber dan untuk mewujudkan kedaulatan data diperlukan pembangunan kapabilitas dari warga negara itu sendiri. Pendekatan yang digunakan seyogyanya mengedepankan pendekatan *people centered*. Negara memiliki tanggung jawab untuk membangun sistem pengelolaan ruang siber yang aman dan demokratis. Dalam hal membangun sistem keamanan siber yang kuat membutuhkan kemampuan negara dalam menyiapkan berbagai sarana dan infrastruktur yang memadai. Infrastruktur internet yang belum merata di seluruh Indonesia merupakan salah satu hal yang esensial dalam pemerataan akses internet bagi seluruh rakyat Indonesia. Negara diharapkan juga lebih mengoptimalkan pemberdayaan industri dalam negeri dan mengembangkan kemampuan putra dan putri terbaik bangsa dalam mengembangkan studi keamanan siber. Kemandirian bangsa tidak akan optimal apabila pemerintah masih memiliki ketergantungan yang besar terhadap industri siber di luar negeri. Kerjasama antara pemerintah dengan perguruan tinggi di Indonesia seyogyanya dapat diintensifkan dalam konteks membangun ekosistem siber yang kuat dan demokratis di Indonesia.

Kemudian, peningkatan kapabilitas warga yang dimaksud adalah meningkatkan kemampuan, wawasan, kesadaran, dan akses yang dimiliki warga negara Indonesia dalam melindungi dan menjaga data-data pribadi miliknya. Warga negara seyogyanya memahami bahwa data adalah properti yang bernilai dan dapat dimanfaatkan untuk kepentingan pemilik data itu sendiri. Hal ini juga bagian dari peran negara dalam membentuk pengelolaan ruang siber yang aman dan demokratis. Warga negara perlu memiliki kemampuan dalam melindungi data-datanya di ruang siber, perlu memiliki kesadaran untuk tidak mudah memberikan informasi datanya di ruang siber, mengetahui hal-hal mendasar dalam membuat password yang kuat dan aman, memahami cara bertransaksi yang aman dan nyaman secara online, dan lain-lain yang terkait dengan ruang siber.

Beberapa konten dalam program kesadaran keamanan siber misalnya seperti manajemen password, perlindungan terhadap serangan virus, pemahaman kebijakan mengenai keamanan siber, menyikapi email asing yang masuk, dan lain-lain.[34] Beberapa hal ini dapat dilakukan agar warga negara memiliki kapabilitas dalam menghadapi permasalahan-permasalahan terkait ruang siber. Dengan kapabilitas yang lebih baik maka warga negara juga memiliki pemahaman yang mumpuni untuk menjaga dan melindungi data-data pribadinya karena data adalah properti yang bernilai.

Pendekatan negara yang lebih dominan belum dapat menjawab persoalan kebocoran data yang seringkali terjadi di republik ini. Pemerintah juga diharapkan mempercepat kehadiran regulasi-regulasi yang dibutuhkan, seperti UU tentang Keamanan dan Ketahanan Siber agar terdapat arah yang jelas terkait pengembangan kebijakan siber

33 Pratama Persadha, "BIN dan Keamanan Siber," *Media Indonesia*, 4 Juli 2017, diakses 10 Desember 2021, http://mediaindonesia.com/read/detail/111325-bin-dan-keamanan-siber

34 Ratri Nur Rohmah, "Upaya Membangun Kesadaran Keamanan Siber Pada Konsumen E-Commerce di Indonesia," *Cendekia Niaga Journal of Trade Development and Studies* 6, no. 1 (Juli 2022): 9.

dan penguatan konteks kedaulatan data di Indonesia. Pembangunan pusat-pusat data perusahaan swasta yang mengelola data-data pribadi warga negara di Indonesia harus ditempatkan di wilayah teritorial Indonesia agar negara memiliki wewenang yang kuat dalam perspektif hukum kedaulatan data.

Kesimpulan

Sistem keamanan siber dan kedaulatan data merupakan pondasi untuk mewujudkan data pribadi di Indonesia. Dalam konteks pembangunannya terdapat dua pilihan, yaitu *state centered* atau *people centered*. Pendekatan berbasis negara akan melekatkan data sebagai suatu konteks *data as capital*. Sedangkan pendekatan berbasis masyarakat lebih melekatkan data pada konteks *data as labor*. Dalam konteks *data as labor* maka data dianggap sebagai milik dari pribadi masing-masing. Data-data pribadi tersebut diharapkan dapat memberi manfaat yang maksimal terhadap masing-masing pemilik data. Sedangkan dalam konteks *data as capital* maka data hanya dianggap sebagai sesuatu yang tidak berguna, sehingga akan diolah menjadi hal yang bermanfaat oleh perusahaan-perusahaan kapitalis. Dalam konteks ekonomi politik konteks *data as labor* lebih memberikan manfaat bagi warga negara dan sejalan dengan nilai-nilai yang demokratis. Dengan demikian menjadi jawaban dari judul penulis di atas, yaitu dalam perspektif ekonomi politik.

Dalam konteks pembangunan keamanan siber dan kedaulatan data di Indonesia lebih didominasi pendekatan negara. Dalam pendekatan negara sangat dibutuhkan regulasi yang mampu mewadahi dan memberikan jaminan keamanan data pribadi tiap warga negara. RUU Perlindungan Data Pribadi belum lama disahkan dan perlu dicermati untuk implementasinya ke depan, sedangkan RUU Keamanan dan Ketahanan Siber hingga saat ditulisnya artikel ini belum disahkan, sehingga menimbulkan kekosongan regulasi. Akibatnya adalah, timbulnya kontradiksi dengan pendekatan negara yang digunakan namun belum terdapat regulasi yang dibutuhkan. Padahal peran utama dari negara adalah menghasilkan regulasi yang dibutuhkan sebagai pedoman. Dalam konteks kedaulatan data nasional posisi Indonesia cukup mengkhawatirkan dikarenakan begitu banyaknya perusahaan-perusahaan teknologi besar yang belum membangun pusat datanya di Indonesia. Berdasarkan hukum kedaulatan data, dengan tidak adanya pusat data dalam wilayah teritorial Indonesia berpotensi menghasilkan daya tawar yang lemah dari negara terhadap perusahaan-perusahaan teknologi besar tersebut, sehingga dilihat dari perspektif ekonomi politik hal ini berpengaruh terhadap kedaulatan data di Indonesia.

Pembangunan kapabilitas warga negara Indonesia terkait keamanan data sangat dibutuhkan. Dalam hal ini, negara memiliki tanggung jawab dalam membentuk sistem keamanan siber untuk memberikan perlindungan data yang aman juga demokratis bagi warga negara Indonesia. Pendekatan *people centered* dengan mengedepankan konteks *data as labor* merupakan solusi untuk mengakselerasi pembangunan keamanan siber dan kedaulatan data di Indonesia. Dengan pendekatan ini akan memberikan kebebasan bagi masing-masing warga negara dalam menjaga data-data pribadi mereka di ruang siber. Kesadaran keamanan data dan informasi berpotensi meningkat sehingga berimplikasi pada peningkatan kapabilitas warga negara terkait proteksi data pribadinya. Data merupakan hal yang sangat bernilai, sudah seyogyanya proteksi keamanan data untuk dioptimalkan. Dengan pembangunan kapabilitas warga negara dapat mewujudkan pembangunan keamanan siber dan kedaulatan data di republik ini.

DAFTAR PUSTAKA

Aji, M. Prakoso, Jerry Indrawan. *Cyberpolitics: Perspektif Baru Memahami Politik Era Siber*. Depok: Rajawali Pers, 2019.

Anjani, Noor Halimah. "Perlindungan Keamanan Siber di Indonesia," *CIPS Ringkasan Kebijakan* 9 (Maret 2021): 1.

Ardiyanti, Handrini. "Cyber Security dan Tantangan Pengembangannya di Indonesia." *Jurnal Politica* 5, no 1 (Juni 2014): 98.

Bakhri, Syaiful. *Ilmu Negara: Dalam Pergumulan Filsafat, Sejarah dan Negara Hukum*. Depok: Rajawali Pers, 2018.

Caporaso, James A, David P Levine. *Teori-Teori Ekonomi Politik*. Yogyakarta: Pustaka Pelajar, 2008.

Chotimah, Hidayat Chusnul, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara," *Jurnal Politica* 10, no. 2 (November 2019): 122-123.

CNN Indonesia. "Jaringan BIN dan Kementerian Dilaporkan Dibobol Hacker China." *CNN Indonesia*, 12 September 2021. Diakses 10 Desember 2021. https://www.cnnindonesia.com/nasional/20210912112723-20-693110/jaringan-bin-dan-kementerian-dilaporkan-dibobol-hacker-china.

CNN Indonesia, "RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan." *CNN Indonesia*, 1 Juli 2022. Diakses 28 September 2022. https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan#:~:text=Jakarta%2C%20CNN%20Indonesia%20%2D%2D,malware%20dengan%20modus%20meminta%20tebusan

DPR-RI. "Naskah Akademik Rancangan Undang-Undang Tentang Keamanan Dan Ketahanan Siber." *DPR-RI*. Diakses 12 Desember 2021. https://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf.

Fischer, Eric. "Cybersecurity Issues and Challenges: In Brief". *Congressional Research Service Report*, 12 Agustus 2016.

Gustiani, Witri, "Terjadi 1,6 Miliar Serangan Siber Sepanjang 2021, Bagaimana dengan 2022 dan Kemunculan Bjorka?" *Pikiran Rakyat*, 27 September 2022. Diakses 28 September 2022. https://www.pikiran-rakyat.com/nasional/pr-015583077/terjadi-16-miliar-serangan-siber-sepanjang-2021-bagaimana-dengan-2022-dan-kemunculan-bjorka

Indrawan, Jerry. "Cyberpolitics sebagai Perspektif Baru Memahami Politik di Era Siber." *Jurnal Politica* 10, no. 1 (Mei 2019): 7-8.

Indrawan, Jerry, Efriza, dan Anwar Ilmar. "Kehadiran Media Baru (New Media) dalam Proses Komunikasi Politik." *Medium Jurnal Ilmiah Fakultas Ilmu Komunikasi Universitas Islam Riau* 8, no. 1 (Juni 2020): 2.

Munir, Nudirman. *Pengantar Hukum Siber di Indonesia*. Depok: Rajawali Pers, 2017.

Ngazis, Amal Nur. "Badan Siber: 36 Juta Malware Serang Situs Penting Indonesia." *Viva*, 12 Desember 2018. Diakses 12 Desember 2021. https://www.viva.co.id/digital/ digilife/1102720-badan-siber-36-juta-malware-serang-situs-penting-indonesia.

Persadha, Pratama. "BIN dan Keamanan Siber." *Media Indonesia*, 4 Juli 2017. Diakses 10 Desember 2021. http://mediaindonesia.com/read/detail/111325-bin-dan-keamanan-siber.

Prabowo, Wisnu Handi, Satriya Wibawa, dan Fuad Azmi. "Perlindungan Data Personal Siber di Indonesia." *Padjadjaran Journal of International Relations* 1, no. 3 (Januari 2020): 222-223, 227, dan 229.

Rohmah, Ratri Nur, "Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia," *Cendekia Niaga Journal of Trade Development and Studies* 6, no. 1 (Juli 2022): 9.

Schmidt, Nikola. *Cyber Security*, dalam *Introduction to Security Studies*, ed. Robert Ondrejcsak, Bratislava: Center for European and North Atlantic Affairs, 2014.

Sen, Amartya. *Development as Freedom*. New York: Alfred A. Knopf, 1999.

Sudibyo, Agus. *Jagat Digital: Pembebasan dan Penguasaan*. Jakarta: KPG, 2019.

Sumartias, Suwandi (Ed). *Keamanan Siber dan Pembangunan Demokrasi di Indonesia*. Jakarta: Pusat Penelitian Badan Keahlian DPR RI dan Intrans Publishing, 2018.

Utami, Mirsya Anandari, "5 Kasus Serangan Siber yang Pernah Terjadi di Indonesia Sebelumnya." *Okezone*, 21 September 2022. Diakses 28 September 2022. https://techno.okezone.com/read/2022/09/21/54/2672211/5-kasus-serangan-siber-yang-pernah-terjadi-di-indonesia-sebelumnya

Yuniarti, Siti dan Erni Herawati. "Analisis Hukum Kedaulatan Digital Indonesia." *Pandecta Jurnal Penelitian Ilmu Hukum* 15, no. 2 (Desember 2020): 159-160.

Yusuf, A Muri. *Metode Penelitian: Kuantitatif, Kualitatif & Penelitian Gabungan*. Jakarta: Kencana, 2017