**PERAN BADAN SIBER DAN SANDI NEGARA DALAM KASUS SERANGAN
SIBER YANG MENGAKIBATKAN KEBOCORAN DATA PRIBADI PUSAT
DATA NASIONAL SEMENTARA 2 (PDNS2)**

Fachrudin Sembiring dan Figo Mandela Pattihahuan

Fakultas Hukum, Universitas Katolik Indonesia Atma Jaya

Jl. Jenderal Sudirman RT 02 RW 04 No. 51, Karet Semanggi, Jakarta 12930

Corresponding Author: fachrudin.sembiring@atmajaya.ac.id

ABSTRAK

Perkembangan teknologi menjadi semakin masif di kehidupan manusia. Teknologi membawa begitu banyak kemanfaatan yang dapat manusia rasakan dan gunakan. Akan tetapi, teknologi juga datang dengan hal-hal negatif. Pada tanggal 20 Juni 2024, server PDNS2 yang berada di Surabaya, mengalami serangan siber yang diidentifikasi sebagai serangan siber *ransomware* buatan kelompok peretas Brain Cipher. Terdapat beberapa permasalahan yang muncul dari kasus tersebut. Pertama, adanya tidak jelas mengenai siapa lembaga negara yang bertanggung jawab terhadap insiden siber ini. Kedua, adanya ego-sektoral terhadap penyelenggaraan keamanan siber di Indonesia. Ketiga, terdapat kekosongan hukum terkait keamanan siber yang menyeluruh termasuk pengaturan teknis mengenai pengelolaan PDNS. Hasil penelitian menunjukkan bahwa adanya permasalahan sinergitas, kekosongan hukum serta kejelasan tanggung jawab yang berimplikasi pada lemahnya praktik pengamanan di bidang siber di Indonesia. Oleh karena itu, Pemerintah bersama-sama dengan DPR RI wajib untuk bersama-sama melakukan pengamanan siber secara bersama-sama guna memenuhi hak privasi warga negaranya.

Kata Kunci: Badan Siber dan Sandi Negara, Kemkominfo, Data Pribadi, Serangan Siber, Ego Sektoral

ABSTRACT

The development of technology is becoming increasingly massive in human life. Technology brings so many benefits that humans can feel and use. However, technology also comes with negatives. On June 20, 2024, the PDNS2 server in Surabaya experienced a cyberattack and was identified as a ransomware cyberattack made by the Brain Cipher hacker group. There are several problems that arise from this case. First, of clarity regarding which state agency is responsible for this cyber incident. Second, there is an ego-sectoral attitude towards the implementation of cyber security in Indonesia. Third, there is a legal vacuum related to comprehensive cybersecurity including technical arrangements regarding the management of PDNS. The results show that there are problems of synergy, legal vacuum, and clarity of responsibility that have implications for the weak security practices in the cyber sector in Indonesia. Therefore, the Government along with the House of Representative is obliged to jointly carry out cyber security together to fulfill the privacy right of its citizens.

Keywords: *National Cyber and Crypto Agency, Ministry of Communication and Informatics, Personal Data, Cyberattack, Ego-Sectoral.*

A. PENDAHULUAN

Saat ini, teknologi memiliki kegunaan yang sangat banyak dan beragam, baik untuk penyimpanan, pengumpulan data dan sejenisnya. Teknologi memiliki peran yang sangat vital dalam kehidupan manusia. Penyimpanan dan pengumpulan data itu umumnya menyangkut data pribadi seseorang. Data diri merupakan ranah privasi seseorang, dan privasi seseorang merupakan hak asasi yang dimiliki oleh tiap-tiap manusia yang dilahirkan di dunia ini. Dalam era Revolusi Industri 4.0, data pribadi memiliki manfaat yang sangat luar biasa, karena data pribadi merupakan aset terbesar yang dapat digunakan oleh para pelaku usaha untuk mengembangkan bisnisnya dengan cara membaca atau menganalisis bagaimana perilaku dan preferensi konsumen melalui data pribadi yang diperoleh baik secara legal maupun dengan cara ilegal.¹

Walaupun teknologi memberi kemanfaatan yang besar bagi umat manusia, teknologi juga menjadi salah satu media yang digunakan oleh orang-orang tidak bertanggung jawab untuk melakukan kejahatan-kejahatan. Dari segala bentuk kejahatan yang menggunakan teknologi informasi tersebut dinamakan kejahatan siber atau dalam bahasa Inggris dikenal dengan kata *cybercrime*. Salah satu bentuk dari *cybercrime* itu sendiri adalah serangan siber dengan menggunakan *ransomware*.²

Banyak kasus-kasus serangan *ransomware* di luar negeri seperti terhadap: JBS (2021), Kaseya (2021), Springhill Medical Center (2019), Texas Municipality (2019) yang menimbulkan kerugian yang sangat besar. Indonesia sendiri mengalami serangan *ransomware* terbanyak di ASEAN. Pada semester pertama 2024, Indonesia mengalami sebanyak 32.803 serangan *ransomware*. Bank Indonesia pernah mengalami serangan *ransomware* oleh Conti *Ransomware*.³ Oleh karena itu, negara wajib untuk melindungi data pribadi masyarakatnya. Salah satu cara negara melindungi data pribadi warga negaranya adalah dengan memberikan payung hukum dalam bentuk peraturan perundang-undangan atau mendirikan lembaga teknis yang menangani pengelolaan data serta keamanan siber.

¹ Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi" *Al-Wasath Jurnal Ilmu Hukum* 5, No. 1 (2024): 19-32, <https://doi.org/10.47776/alwasath.v2i1.127>

² Budi Hartono, "Ransomware: Memahami Ancaman Keamanan Digital" *Bincang Sains dan Teknologi (BST)* 2, No. 2 (2023): 55-62, <https://doi.org/10.56741/bst.v2i02.353>

³ Yuliansron, "Indonesia Jadi Target Utama *Ransomware* di Asia Tenggara: Begini Cara Lindungi Data Kamu!" Terakhir diubah 20 Des 2024. <https://www.liputan6.com/tekno/read/5842580/indonesia-jadi-target-utama-ransomware-di-asia-tenggara-begini-cara-lindungi-data-kamu>

Namun di Indonesia tata kelola dan tata kerja mengenai urusan-urusan keamanan siber merupakan permasalahan sektoral dan parsial, sehingga membutuhkan kerja sama dan integrasi yang sangat terpadu. Ini menyebabkan celah yang besar bagi ancaman-ancaman siber yang berpotensi menyerang Indonesia. Insiden-insiden kebocoran data di sektor publik acapkali terjadi di Indonesia, hal ini menunjukkan bahwa sebetulnya pemerintah belum siap untuk mengelola data pribadi masyarakatnya. Apabila kita melihat dari lima tahun belakangan sudah ada beberapa kasus kebocoran data di sektor publik, mulai dari kebocoran data pengguna aplikasi eHAC, BPJS Kesehatan, DPT Pemilu KPU, e-KTP, dan PDNS2. Dari kasus-kasus tersebut sampai sekarang belum ada penyelesaian yang secara tuntas oleh pemerintah sebagai pengelola data.⁴

Pada minggu ketiga bulan Juni 2024, tepatnya pada tanggal 20 Juni 2024, server PDNS2 yang berada di Surabaya, mengalami serangan siber yang diidentifikasi sebagai serangan *ransomware* buatan kelompok peretas Brain Cipher. Berdasarkan Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) “Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data dan pemulihan data”. Menurut Pasal 27 ayat (4) Perpres SPBE, Pusat Data Nasional (PDN) digunakan secara *sharing* baik oleh Instansi Pusat maupun Pemerintah Daerah yang saling terhubung. Saat ini PDN sedang dalam proses pembangunan, sehingga dalam pengoperasiannya, Kemkominfo menyelenggarakan Pusat Data Nasional Sementara untuk digunakan selagi menunggu pembangunan PDN rampung. Brain Cipher menyerang server PDNS2 di Surabaya dengan menggunakan *ransomware* dan meminta tebusan uang dengan jumlah sebesar Rp131.600.000.000,00 (seratus tiga puluh satu milyar enam ratus juta rupiah), apabila pemerintah menolak untuk membayar, maka Brain Cipher akan menghapus seluruh data yang tersimpan di server PDNS2. Akan tetapi, pemerintah Indonesia bersikeras untuk tidak memenuhi apa yang diminta oleh Brain Cipher.⁵

⁴ Berdasarkan data yang diperoleh, Indonesia pernah mengalami penyerangan siber dengan jenis serangan siber *ransomware* wannacry pada tahun 2017, yang mengakibatkan kerugian finansial yang cukup besar. *Ransomware* wannacry tersebut menyerang beberapa server rumah sakit seperti Rumah Sakit Dharmais Jakarta dan Rumah Sakit Harapan Kita, sehingga dua rumah sakit tersebut menjadi terganggu operasionalnya. Pada tanggal 23 Agustus 2019, Indonesia pernah juga mengalami gangguan siber yang berdampak pada pelayanan penerbangan di Terminal 3 Bandara Soekarno-Hatta.

⁵ Desty Luthfiani, “Peretas Pusat Data Nasional Minta Tebusan Rp 131 Miliar” Terakhir diubah 24 Juni 2024. <https://www.tempo.co/politik/peretas-pusat-data-nasional-minta-tebusan-rp-131-miliar-46354>

Kebocoran data PDNS2 yang melibatkan Kominfo, BSSN, dan Telkomsigma menunjukkan ketidakjelasan dalam pembagian tanggung jawab di dalam pengawasan data pribadi masyarakat. Dalam situasi seperti ini, masing-masing lembaga cenderung menyalahkan satu sama lain, yang bisa menghambat proses penyelesaian dan pemulihan. Kemkominfo berfokus sebagai pengelola PDNS2 serta pembuat regulasi dan kebijakan, BSSN menangani aspek keamanan siber dan sebagai *leading sector*, dan Telkomsigma sebagai penyedia layanan infrastruktur memiliki tanggung jawab terkait keamanan data yang mereka kelola.⁶

Ketika masalah terjadi, sangat penting untuk adanya koordinasi yang baik di antara ketiga lembaga ini untuk memastikan transparansi dan penanganan yang efektif. Jika situasinya berlanjut tanpa solusi jelas, ini dapat memengaruhi kepercayaan publik terhadap kemampuan mereka dalam melindungi data. Sehingga menciptakan suatu ketidakpastian hukum. Hal tersebut bertentangan dengan Asas-Asas Umum Pemerintahan yang Baik (AAUPB), bahwa Pemerintah harus memberikan kepastian hukum kepada warga negaranya. Permasalahan-permasalahan tersebut menimbulkan pertanyaan yang menarik untuk dianalisis yaitu Bagaimana tanggung jawab Badan Siber dan Sandi Negara (BSSN) dalam kasus kebocoran data Pusat Data Nasional Sementara 2 dan Bagaimana strategi dan upaya mitigasi yang dapat dilakukan oleh Badan Siber dan Sandi Negara terkait serangan siber yang mengakibatkan kebocoran data pribadi.

Dengan demikian, diharapkan dengan dibentuknya lembaga negara yang menyelenggarakan urusan-urusan keamanan siber dan sandi negara seperti BSSN dapat menghadapi berbagai permasalahan dan tantangan yang muncul dalam dunia siber, baik saat ini maupun di masa depan. Selain itu, BSSN juga diharapkan dapat meningkatkan komitmennya dalam bidang keamanan siber untuk menghadapi ancaman-ancaman siber yang berpotensi membahayakan Indonesia.

Badan Siber dan Sandi Negara (BSSN) merupakan salah satu dari sekian lembaga negara yang terbentuk karena perubahan dari lembaga yang bernama Lembaga Sandi Negara yang didirikan oleh negara pada tanggal 4 April 1946. Pada tahun 19 Mei 2017 Lembaga Sandi Negara mengalami perubahan nama menjadi Badan Siber dan Sandi Negara (BSSN) dengan dikeluarkannya Perpres No. 53 Tahun 2017 yang kemudian

⁶ Yusep Ginanjar, "Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara", *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, No.2 (2022): 295-316, <https://doi.org/10.36859/jdg.v7i02.1187>

dicabut dengan dikeluarkannya Peraturan Presiden No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara yang diresmikan oleh Presiden RI ke-7 Joko Widodo.

Dengan dibentuknya Lembaga negara yang membantu jalannya pemerintah di bidang keamanan siber dan sandi seperti BSSN, maka pelaksanaan seluruh tugas dan fungsi terkait persandian yang sebelumnya merupakan wewenang Lembaga Sandi Negara (Lemsaneg) serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan serta infrastruktur telekomunikasi yang berada di Kemkominfo dilaksanakan sepenuhnya oleh BSSN. Sebagai Lembaga negara, BSSN memiliki tugas dan wewenang untuk melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan sebagaimana yang dimaksud dalam Pasal 2 Perpres No. 28 Tahun 2021.

Kemudian dalam Pasal 3 Perpres No. 28 Tahun 2021, disebutkan bahwa BSSN memiliki beberapa fungsi yaitu:

- a) perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi;
- b) pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi;
- c) penyusunan norma, standar, prosedur, dan kriteria di bidang persandian;
- d) pelaksanaan bimbingan teknis dan supervisi di bidang persandian;
- e) koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN;
- f) pengelolaan barang milik negara yang menjadi tanggung jawab BSSN;
- g) pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN
- h) pengawasan atas pelaksanaan tugas di lingkungan BSSN.

Adapun pada Bab III Perpres No. 28 Tahun 2021 yang terdiri dari Pasal 33 sampai dengan Pasal 41 mengatur mengenai Tata Kerja BSSN dalam penyelenggaraannya sebagai lembaga negara yang bergerak di bidang keamanan siber dan sandi. Pasal 38 Perpres No. 28 Tahun 2021 memastikan bahwa “Setiap unsur di lingkungan BSSN dalam melaksanakan tugas dan fungsi harus menerapkan prinsip koordinasi, integrasi, dan sinkronisasi baik dalam lingkungan BSSN maupun dalam hubungan antar kelembagaan dengan lembaga lain terkait”. Di dalam pasal tersebut, dijelaskan bahwa dalam melaksanakan tugas dan fungsi harus diperlukannya kerja sama yang baik dengan

lembaga-lembaga lain yang terkait dengan urusan-urusan pemerintahan di bidang keamanan siber dan sandi negara.

B. PEMBAHASAN

1. Tanggung Jawab Kelembagaan Negara dalam Kasus PDNS2

Apabila kita melihat pada kasus kebocoran data pribadi dari server Pusat Data Nasional Sementara 2 (PDNS2), maka seharusnya tidak ada lagi yang saling lempar tanggung jawab antara BSSN, Kominfo, dan Telkomsigma. Karena seharusnya BSSN harus bisa berkoordinasi dengan lembaga lain berdasarkan Pasal 38 Perpres No. 28 Tahun 2021 tersebut. Dalam argumennya, BSSN menyatakan bahwa tanggung jawab untuk menjaga keamanan siber adalah tanggung jawab bersama. BSSN mengatakan menurut Pasal 3 PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan “Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.”

Oleh karena itu BSSN menilai bahwa tanggung jawab dari serangan siber adalah tanggung jawab bersama, BSSN menyatakan bahwa seharusnya kebocoran data pribadi PDNS2 ini menjadi tanggung jawab antar lembaga yang berwenang. Pernyataan yang dilontarkan oleh BSSN itu menimbulkan masalah yang cukup serius, apabila dikatakan bahwa serangan siber merupakan tanggung jawab bersama dalam konteks kasus kebocoran data pribadi PDNS2, maka dapat disimpulkan bahwa sebetulnya tidak ada urgensi untuk membentuk lembaga BSSN, karena masing-masing penyelenggara elektronik akan melakukan upaya-upaya perlindungan data pribadi berdasarkan “*best practice*”. Terlebih dalam kasus serangan siber terhadap kebocoran data PDNS2, itu merupakan ranah pemerintah dalam menjaga data pribadi warga negaranya selaku Pengendali Data dan Prosesor Data.

Akan tetapi, ada argumentasi lain yang mendukung pernyataan dari BSSN. Jika kita menggunakan sudut pandang yang menggunakan asas hukum sebagai dasar untuk melaksanakan peraturan perundang-undangan, maka terdapat asas yang mengatur pelaksanaan peraturan perundang-undangan, yaitu asas *lex superior derogat lex inferior* yang artinya peraturan perundang-undangan yang lebih tinggi dapat mengesampingkan peraturan yang lebih rendah. Dalam kasus ini, argumen dari BSSN dapat dinilai benar, karena dengan merujuk Pasal 3 PP No. 71 Tahun 2019 memang dikatakan bahwa

tanggung jawab terhadap suatu kebocoran data atau terhadap serangan siber adalah merupakan tanggung jawab bersama. Berdasarkan UU No. 12 Tahun 2011 Pembentukan Peraturan Perundang-undangan, dalam hierarki peraturan perundang-undangan pada Pasal 7, Peraturan Pemerintah kedudukannya lebih tinggi daripada Peraturan Presiden, sehingga dalam kasus ini BSSN merujuk PP No. 71 Tahun 2019 sebagai dasar daripada pelaksanaan tugas, pokok, dan fungsi BSSN dalam kaitannya terhadap serangan *ransomware* PDNS2.

Kendati demikian, argumen BSSN yang merujuk PP No. 71 Tahun 2019 tersebut tidak mengesampingkan tugas utamanya, karena sudah dijelaskan menurut Pasal 2 Perpres No. 28 Tahun 2021, bahwa BSSN memiliki tugas utama sebagai *leading sector* di bidang keamanan siber di Indonesia dalam rangka membantu presiden dalam menyelenggarakan pemerintahan. Tidak bisa BSSN hanya melempar tanggung jawab untuk mengamankan siber kepada lembaga lain, karena hal itu juga akan bertentangan dengan Pasal 38 Perpres No. 28 Tahun 2021, yang menyatakan bahwa harus ada sinkronisasi baik dalam lingkungan BSSN ataupun lembaga lain yang terkait dengan tugas dan fungsi yang dijalankan oleh BSSN.

Oleh karena itu, seharusnya BSSN dengan Kemkominfo bisa saling bersinergi untuk bertanggung jawab dan menanggulangi kasus kebocoran data pribadi PDNS2. Karena, apabila dibiarkan terus seperti ini, masing-masing lembaga negara akan terus menghindar dari tanggung jawabnya dan akan terus menerapkan ego sektoral dalam menjalankan tugas pokok dan fungsinya. Sehingga tidak ada kejelasan, kepastian, serta keadilan bagi masyarakat Indonesia. Tanggung jawab terhadap keamanan siber tetap merupakan tanggung jawab dari BSSN sebagaimana yang dimaksud dalam visi misi atau semangat pembentukan BSSN, akan tetapi BSSN juga harus dibantu dengan Kementerian/Lembaga/Satuan Kerja Perangkat Daerah/Institusi (K/L/D/I) terkait.

Dalam praktik penyelenggaraan pemerintahan, acapkali terdapat hambatan-hambatan dalam birokrasinya. Hambatan-hambatan dalam penyelenggaraan pemerintahan itu sudah sering dan lama terjadi di Indonesia. Penyebab utama daripada hambatan tersebut adalah permasalahan ego sektoral sehingga menyebabkan tidak sinerginya hubungan antar lembaga negara. Ego sektoral atau tidak sinerginya tersebut dapat muncul juga dari kurangnya atau tidak adanya upaya-upaya koordinasi serta komunikasi yang jelas oleh lembaga-lembaga negara. Ego sektoral sering juga disebut

sebagai mentalitas cerobong atau juga yang biasa disebut dengan *silo mentality*. Mentalitas cerobong adalah pola pikir dan tindakan yang tidak ingin berbagi informasi atau bekerja sama dengan pihak lain dalam suatu negara. Ego sektoral atau mentalitas cerobong biasanya dimulai karena adanya persaingan baik internal ataupun eksternal dalam suatu lembaga sehingga dapat menyebabkan komunikasi yang tidak baik yang berujung pada kegagalan untuk memahami satu dengan yang lain.⁷

2. Upaya Integrasi BSSN, Kominfo dan Telkomsigma dalam Pencegahan Kebocoran Data Pribadi

Berkaca pada kasus peretasan PDNS2 yang menyebabkan kebocoran data pribadi, maka seharusnya BSSN, Kemkominfo, serta Telkomsigma harus saling berintegrasi dan berkoordinasi antar lembaga. BSSN, Kemkominfo, serta Telkomsigma harus melakukan komunikasi dan koordinasi secara rutin untuk mengambil tindakan atau merumuskan suatu kebijakan yang berkenaan dengan pengelolaan data pribadi masyarakat. Tidak bisa masing-masing lembaga hanya bekerja sendiri-sendiri, karena data pribadi merupakan hal yang sangat penting dan wajib untuk dijaga keamanannya. Kasus PDNS2 membuktikan bahwa apabila lembaga-lembaga negara saling menerapkan ego sektoral atau *silo mentality*, maka itu akan membawa ketidakharmonisan dalam menangani keamanan siber di Indonesia, yang seharusnya lembaga-lembaga negara itu saling bekerja sama untuk mengatasi serangan siber, menjadi saling lempar tanggung jawab dan saling menyalahi satu sama lain. Tidak elok apabila kita melihat persilatan antar pemangku kepentingan, padahal yang sebetulnya harus diutamakan adalah keamanan data pribadi masyarakat, bukan untuk menyelamatkan wajah masing-masing lembaga negara.

Ego sektoral memberikan dampak yang cukup serius terhadap penyelenggaraan pemerintahan apabila berkaitan dengan keamanan siber. *Pertama*, ego sektoral sudah pasti akan menyebabkan adanya tumpang tindih peraturan, program, serta Tugas Pokok dan Fungsi (Tupoksi) antar lembaga negara. Pada kasus PDNS2 ini, sudah terbukti bahwa terdapat tumpang tindih peraturan dan pelaksanaan teknisnya, Contohnya adalah tumpang tindih antara PP No. 71 Tahun 2019 dengan Perpres No. 28 Tahun 2021. Menkominfo berpendapat mengenai keamanan siber dan pengelolaan data merupakan ranah atau domain dari BSSN, lain dengan BSSN yang mengatakan ini merupakan kewenangan dan

⁷Tedo Hindami Guna, "Breaking down barriers: Overcoming silo mentality in bureaucratic reform" *Journal of Sustainability, Society, and Eco-Welfare* 2, No. 1 (2024): 16–28, <https://doi.org/10.61511/jssew.v2i1.2024.884>

tanggung jawab bersama. Artinya terdapat tumpang tindih yang serius dalam mengatasi keamanan siber. *Kedua*, masing-masing lembaga memiliki prioritas yang berbeda menyebabkan tidak sinergi dalam menyelenggarakan pemerintahan, lembaga-lembaga negara sudah pasti akan menjalankan program yang sekiranya akan memberikan keuntungan bagi mereka.

Ketiga, ketika suatu insiden serangan siber terjadi maka akan memunculkan keterbatasan dalam merespon serangan tersebut. Jika ada kebocoran data pribadi di sebuah negara yang melibatkan data yang dikelola oleh beberapa sektor, dalam kasus ini yang mengelola adalah BSSN, Kemkominfo, dan Telkomsigma, sehingga masing-masing sektor mungkin hanya fokus pada data yang mereka kelola sendiri tanpa bekerja sama dalam mitigasi atau pemberitahuan yang menyeluruh kepada korban yaitu masyarakat. Fakta yang terungkap saat rapat DPR RI dalam rangka mendengarkan keterangan Kemkominfo dan BSSN, ternyata selama ini BSSN tidak pernah dilibatkan pada saat proses desain server Pusat Data Nasional (PDN) dan Pusat Data Nasional Sementara (PDNS). Proses desain PDN dan PDNS dibuat secara tertutup oleh Kemkominfo RI. Walaupun BSSN dianggap sebagai *leading sector* dalam penanganan keamanan siber dan data, Kemkominfo RI harus tetap menjalin kerja sama atau kolaborasi yang aktif kepada BSSN, sehingga dalam pengambilan keputusan atau pembuatan program, BSSN selalu dilibatkan dan bisa menjalankan tupoksinya secara maksimal.⁸ Dari ketiga dampak tersebut kemudian akan memberikan dampak secara tidak langsung juga terhadap kepercayaan masyarakat kepada pemerintah. Ketika masyarakat merasa bahwa data pribadi mereka tidak dikelola dengan baik, kepercayaan terhadap pemerintah dapat menurun. Jika masyarakat melihat bahwa berbagai sektor tidak bekerja sama secara baik dalam melindungi data pribadi, mereka mungkin merasa bahwa data mereka tidak aman.

Untuk mengatasi permasalahan-permasalahan ketidakharmonisan antar lembaga yang disebabkan oleh ego sektoral atau *silo mentality* ini, maka pemerintah harus berbenah diri untuk mencapai sinergitas antar lembaga negara. Pemerintah perlu untuk menyusun suatu regulasi yang mengharmonisasikan peraturan-peraturan teknis untuk mengatasi permasalahan-permasalahan siber ke depannya, pemerintah harus memberikan kewenangan yang jelas kepada lembaga mana yang mengelola data pribadi dan

⁸ Eka Yudha Saputra, “Benarkah BSSN Abai Melindungi Pusat Data Nasional” Terakhir diubah 26 Juni 2024, <https://www.tempo.co/politik/abai-bssn-pusat-data-nasional-410023>

bertanggung jawab apabila ada serangan siber. Artinya, pemerintah bersama-sama dengan DPR RI harus menciptakan Undang-Undang mengenai Keamanan Siber. Peraturan perundang-undangan di tingkat Undang-Undang perlu diterbitkan untuk mengharmonisasi peraturan dan wewenang tiap-tiap lembaga yang berkaitan dengan keamanan siber, sehingga semua lembaga yang menangani keamanan siber ini bekerja dalam satu payung hukum yang sama, tidak ada lagi lempar tanggung jawab yang beralasan perbedaan peraturan yang digunakan.

Walaupun sulit untuk mengatasi permasalahan ketidaksinergian yang mengakar, Pemerintah Republik Indonesia perlu untuk mengubah sistem serta budaya kelembagaan, kepemimpinan, koordinasi, serta cara pengambilan keputusan di level kepentingan publik. Langkah-langkah tersebut harus diintegrasikan dan melibatkan kolaborasi yang aktif antar sektor, yang bertujuan untuk memastikan tindakan dan kebijakan publik yang lebih efektif, efisien, dan adil.

Dengan demikian, BSSN, Kemkominfo, dan Telkomsigma tidak boleh lagi untuk saling melempar tanggung jawab apabila ada kasus kebocoran data yang disebabkan oleh serangan siber. Kejadian seperti bocornya data pribadi PDNS2 ini menunjukkan betapa pentingnya kolaborasi antar lembaga dan sektor yang terlibat dalam keamanan siber, terutama ketika menyangkut perlindungan data pribadi warga negara. Sikap yang mengarah pada saling tuding atau menghindari dari tanggung jawab justru akan memperburuk situasi dan menambah kerugian, baik materiil maupun reputasi.

Kebocoran data di sektor publik khususnya pada kasus PDNS2 menjadi sorotan yang hangat bagi masyarakat. Seperti yang sudah dijelaskan sebelumnya, bahwa data pribadi merupakan aset dengan nilai ekonomi yang tinggi pada zaman revolusi industri 4.0 ini. Insiden kebocoran data yang menimpa PDNS2 menunjukkan bahwa ada urgensi untuk melindungi data pribadi masyarakatnya, dan menunjukkan bahwa lemahnya pertahanan Indonesia terhadap serangan siber. Bukan hanya terhadap kebocoran data pribadi saja, akan tetapi serangan siber dari *Ransomware* ini berdampak terhadap pelayanan publik, Walaupun serangan siber di masa kini tak terelakkan, akan tetapi itu bukan menjadi alasan bahwa Indonesia tidak bisa untuk membendung serangan siber dari dalam negeri maupun dari luar negeri. BSSN telah menyusun strategi untuk melindungi dan mengatasi apabila terjadi serangan siber di Indonesia, strategi yang disusun tersebut mengacu pada pedoman yang dibuat oleh *Global Cybersecurity Index (GCI)*. Menurut

GCI terdapat lima aspek terkait apa saja yang menjadi landasan untuk menyusun upaya-upaya mitigasi serta strategi dalam meningkatkan keamanan siber khususnya di Indonesia, yaitu aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas, dan yang terakhir merupakan aspek kerja sama.⁹

Aspek legal berbicara mengenai pengukuran terhadap hukum dan peraturan yang berlaku terkait kejahatan siber dan keamanan siber. Hukum sudah pasti akan menjamin kekuatan keamanan siber suatu negara. Hukum dijadikan alat untuk mencegah dan memitigasi ancaman siber. Walaupun saat ini sudah ada Undang-Undang yang mengatur mengenai Perlindungan data pribadi yaitu dengan dikeluarkannya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), akan tetapi itu belum cukup untuk mengatasi keamanan siber di Indonesia, karena UU PDP hanya berfokus pada pelindungan data pribadi saja, sedangkan yang dibutuhkan saat ini pasca terjadinya gelombang serangan siber di Indonesia adalah UU Keamanan Siber. Permasalahan utama dari keamanan siber di Indonesia adalah tidak ada peraturan di tingkat Undang-Undang yang mengatur mengenai keamanan siber secara jelas, sehingga ini membuat tumpang tindih antara peraturan satu dengan peraturan lainnya.

Apabila terdapat suatu kerangka hukum yang dibuat maka hal tersebut dapat dijadikan landasan atau pedoman bagi BSSN dalam menjalankan tugasnya sebagai lembaga yang menjadi *leading sector* atau koordinator dalam menangani keamanan siber di Indonesia. Pemerintah bersama-sama dengan DPR RI harus membahas, memasukkan ke dalam Program Legislasi Nasional untuk mengesahkan UU Keamanan Siber secepatnya guna melindungi keamanan siber bagi masyarakat Indonesia. Selain itu terdapat kekosongan hukum di mana tidak ada kewajiban untuk melakukan pengembangan teknologi terkait keamanan siber PDNS, pada Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia (SDI) tidak diatur secara spesifik mengenai pengembangan, teknis, dan lain-lain, pada Perpres SDI hanya diatur mengenai definisi serta penggunaannya saja.

Oleh karena itu Pemerintah harus segera mengisi kekosongan hukum tersebut dengan mengeluarkan peraturan perundang-undangan yang baru, yang mewajibkan suatu K/L/D/I untuk mengembangkan teknologi pengamanan siber di PDNS. Kendati terdapat

⁹ Damar Apri Sudarmadi dan Arthus Josias Simon Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia", *Jurnal Kajian Strategik Ketahanan Nasional* 2, No. 2 (2019): 163-183, <https://doi.org/10.7454/jkskn.v2i2.10028>

adagium hukum berbunyi “*Het recht hink achter de feiten an*” yang berarti hukum itu selalu tertinggal dari peristiwa yang diaturnya, bukan berarti hukum hanya sebagai aksi reaksi saja, seharusnya pembuat undang-undang beserta pemangku kepentingan dapat melakukan prediksi (*forecasting*) terhadap kejadian-kejadian yang sekiranya dapat merugikan negara, kemudian dapat dicegah dengan dibuatnya peraturan perundang-undangan.

Aspek teknis berbicara mengenai pengukuran implementasi kemampuan teknis melalui lembaga-lembaga dan sektor tertentu. Bersama-sama dengan aspek hukum, aspek teknis juga sangat berpengaruh besar dalam keamanan dan ketahanan terhadap serangan siber. Mengenai aspek teknis, aspek teknis diukur berdasarkan beberapa elemen yaitu kompetensi individu, proses, standar operasional prosedur, serta teknologi yang mendukungnya. Dari beberapa elemen itu digunakan untuk menunjang pencegahan, pengamanan, dan respon terhadap insiden serangan siber. Aspek teknis dapat diukur dengan menggunakan enam indikator yaitu:

1. Tim Tanggap Darurat Komputer/*Cyber Emergency Response Team* (CERT) Nasional
2. Tim Tanggap Darurat Komputer/*Cyber Emergency Response Team* (CERT) Pemerintah
3. Tim Tanggap Darurat Komputer/*Cyber Emergency Response Team* (CERT) Sektoral
4. Standar keamanan siber bagi organisasi
5. Standar dan sertifikasi bagi profesional bidang keamanan siber
6. Perlindungan daring bagi anak

Indonesia melalui BSSN sudah membentuk (CERT) yang kemudian BSSN telah meningkatkan Tim Tanggap Darurat Komputer tersebut menjadi Tim Tanggap Insiden Siber/*Computer Security Incident Response Team* (CSIRT) berdasarkan Peraturan BSSN No. 10 Tahun 2020. CSIRT sendiri merupakan tim yang berisikan sekelompok orang yang memiliki peran untuk bertanggung jawab dalam menangani insiden-insiden siber yang terjadi. Apabila terjadi suatu insiden siber, maka CSIRT akan membantu untuk menentukan insiden siber apa yang terjadi dan kemudian membantu untuk mengambil

langkah yang diperlukan untuk mengatasi insiden siber tersebut.¹⁰ Pada Tahun 2019, CSIRT dikembangkan lagi berdasarkan Keputusan Kepala BSSN No. 199 Tahun 2019, menjadi Tim Tanggap Insiden Siber Pemerintah/*Government Computer Security Incident Response Team (Gov-CSIRT)* yaitu CSIRT yang berfokus pada sektor pemerintah. Gov-CSIRT memiliki tujuan yaitu Pertama, membangun, mengoordinasikan, mengolaborasi dan mengoperasikan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah. Kedua, membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah, Ketiga, membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah. Keempat, yaitu mendorong pembentukan Tim Tanggap Insiden Siber/*Computer Security Incident Response Team* pada sektor pemerintah.¹¹ Dalam Rapat di DPR RI terkait serangan siber PDNS2 yang mengakibatkan kebocoran data pribadi masyarakat, BSSN mengungkapkan bahwa ada ketidaksiapan dan keterbatasan anggaran yang dialokasikan untuk keamanan siber. Oleh karena itu, Negara harus memberikan anggaran lebih untuk keamanan siber.

Aspek organisasi berbicara mengenai pengukuran organisasi dalam pengimplementasian keamanan siber. Pengukuran terhadap organisasi atau lembaga cukup diperlukan untuk melihat sejauh mana implementasi keamanan siber diterapkan, karena organisasi atau lembaga menjadi penting untuk mengarahkan dan menjadi acuan keamanan siber di suatu negara. Di Indonesia, berdasarkan PP 71 Tahun 2019 dan dibentuknya BSSN melalui Perpres No. 28 Tahun 2021, maka yang bertanggung jawab adalah BSSN. Kemudian terkait parameter aspek organisasi mengenai strategi keamanan siber nasional, Indonesia sudah memiliki Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Serta di BSSN sendiri juga telah membuat Peraturan tambahan dengan Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber.

¹⁰ Ana Najiyya & Stepiani Sisca Wulandari, "Eksplorasi Implementasi Kebijakan Pembentukan Computer Security Incident Response Team (Csirt) di Kementerian Perdagangan: Sebuah Studi Kualitatif" *Jurnal Riset Akuntansi Multiparadigma* 10, No. 1 (2023): 50-55. <https://doi.org/10.30743/akuntansi.v10i1.7246>

¹¹ Prabaswari, Muhamad Alfikri, Irdam Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah" *Matra Pembaruan Jurnal Inovasi Kebijakan* 6, No. 1 (2022): 1-13, <https://doi.org/10.21787/mp.6.1.2022.1-13>

Aspek pengembangan kapasitas berbicara mengenai pengukuran kesadaran, pelatihan, pendidikan untuk keamanan siber. Apabila aspek hukum, aspek teknis, serta aspek organisasi sudah terpenuhi dan sudah terimplementasi dengan baik, maka selanjutnya adalah melakukan pengembangan terhadap kapasitas sumber daya manusia yang bekerja di dalamnya. Pengembangan kapasitas merupakan kunci untuk membangun suatu ekosistem keamanan siber yang kuat di dalam suatu negara. Apabila suatu negara tidak didukung oleh kemampuan-kemampuan sumber daya manusia yang memiliki keterampilan siber yang baik, maka akan membahayakan pertahanan suatu negara di bidang siber. Pada Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia khususnya di Pasal 29 ayat (2), dinyatakan bahwa Rencana Aksi Satu Data Indonesia dapat mencakup pengembangan sumber daya manusia yang kompeten. Walaupun dalam frasa Pasal 29 ayat (2) menggunakan kata “dapat” yang artinya tidak ada kewajiban di situ, akan tetapi dalam perencanaannya tetap ada upaya untuk mengembangkan sumber daya manusia yang kompeten. Kendati demikian, seharusnya pengembangan sumber daya manusia yang kompeten merupakan kewajiban yang harus dipenuhi, maka diharapkan adanya perbaikan terhadap Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia

Aspek kerja sama berbicara mengenai pengukuran kerja sama antar lembaga, antar negara, ataupun perusahaan. BSSN berdasarkan Pasal 38 Perpres 28 Tahun 2021 sudah berkewajiban untuk menjalin kolaborasi antar BSSN itu sendiri dan dengan lembaga yang terkait dengan keamanan siber ini, misalnya adalah dengan Kemkominfo, Telkomsigma, dan lain-lainnya yang berkaitan dengan keamanan siber. BSSN juga sering memberikan pelatihan kepada sektor pemerintah maupun swasta . Selain di lingkup nasional, Indonesia melalui BSSN telah menjalin kerja sama dengan beberapa negara baik dalam bentuk kerja sama bilateral maupun multilateral. Contohnya adalah Pada tahun 2018 BSSN menjalin kerja sama dengan Pemerintah Australia yaitu *Department of Foreign Affairs*, yang dalam kerja sama bertujuan untuk meningkatkan keamanan siber di Indonesia dengan cara bertukar informasi mengenai praktik terbaik (*best practice*) yang dilakukan.¹²

Sebagai lembaga negara yang menjadi *leading sector* di bidang keamanan siber di Indonesia, maka BSSN memiliki upaya-upaya mitigasi yang harus dilakukan apabila

¹² Muhammad Rafi Shidiqqe & Mansur Juned, “Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)”. *Journal of Social and Political Sciences* 6, No. 4 (2023): 215-224. <https://doi.org/10.31014/aior.1991.06.04.457>

terdapat serangan siber yang mengakibatkan kebocoran data pribadi masyarakat. Pertama, BSSN bekerja sama dengan Kemkominfo serta vendor harus melakukan audit, kajian, serta *penetration stress test* terhadap keamanan siber dan infrastruktur yang menunjang sebagai bentuk dari perlindungan hukum data pribadi. Kedua, BSSN harus membuat rencana untuk pemulihan data terkait insiden serangan siber. Permasalahan utama pada kasus insiden siber yang mengakibatkan kebocoran data pribadi PDNS2 adalah data pribadi masyarakat tersebut terenkripsi atau terkunci sehingga pengendali data dan pengelola data tidak bisa mengaksesnya. Data pribadi tersebut kemudian dijadikan sandera oleh kelompok peretas Brain Cipher, sehingga apabila pemerintah tidak membayar uang tebusan senilai Rp131.600.000.000,00 (seratus tiga puluh satu miliar enam ratus juta rupiah) maka Brain Cipher akan menghapus file yang berisikan data pribadi tersebut. BSSN harus terus mengaudit dan mengkaji Kementerian/Lembaga/Satuan Kerja Perangkat Daerah/Institusi yang menggunakan PDNS2 harus selalu mencadangkan data secara berkala. Ketiga, saat insiden siber terjadi, BSSN wajib untuk bekerja sama dengan negara lain yang pengalamannya dalam menangani insiden siber khususnya insiden serangan siber dengan jenis *ransomware*, sudah lebih ahli dibandingkan dengan Indonesia.¹³

C. PENUTUP

Data pribadi menjadi aset berharga dengan nilai ekonomi yang tinggi sehingga dapat digunakan oleh siapa saja, baik secara legal maupun ilegal, sehingga perlindungan terhadap data pribadi menjadi hal yang sangat penting di era Revolusi Industri 4.0 ini. Berdasarkan Pasal 28G UUD NRI Tahun 1945, privasi merupakan hak yang harus dihormati, dipenuhi, dan dijaga. Oleh karena itu, Pemerintah harus melindungi data pribadi warga negaranya guna memenuhi Hak Asasi Manusia. Dalam melindungi data pribadi, tentunya harus diimbangi dengan keamanan siber yang mumpuni, artinya menjadi tugas pemerintah untuk selalu memastikan bahwa terdapat keamanan siber yang kuat. Pemerintah melalui BSSN harus selalu mengaudit atau mengkaji terkait keamanan siber khususnya di sektor publik. BSSN harus memastikan K/L/D/I yang menjadi pengelola data pribadi masyarakat harus patuh dengan peraturan perundang-undangan

¹³ Aryojati Ardipandanto, "Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber", *Info Singkat* 16, No. 13 (2024): 7-9

yang berlaku seperti UU PDP, UU ITE beserta peraturan turunannya, Perpres SDI, Perpres SPBE, dan lain-lain terkait perlindungan data pribadi dan keamanan siber. Selain itu, BSSN dan Kemkominfo harus saling berkesinambungan atau bekerja sama dalam menangani keamanan siber di Indonesia.

BSSN juga harus memperkuat dan memenuhi lima aspek keamanan siber berdasarkan pengukuran skala *Global Cybersecurity Index (GCI)*, yaitu aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas, dan yang terakhir merupakan aspek kerja sama. Apabila lima aspek ini sudah terpenuhi, maka pertahanan dan keamanan siber di Indonesia akan sulit untuk memiliki celah serangan siber. Walaupun serangan siber di masa sekarang tak terelakkan, ketika lima aspek keamanan siber tersebut sudah terpenuhi dengan baik, maka Pemerintah melalui BSSN dapat mengatasi serangan siber tersebut dengan sigap.

Penulis memiliki pendapat bahwa BSSN harus selalu dilibatkan dalam proses pendesainan tiap-tiap pembangunan infrastruktur penunjang keamanan siber di Indonesia. Penulis berharap untuk ke depannya tidak ada lagi ego-sektoral dalam menangani keamanan siber, sehingga menciptakan pertahanan siber yang kuat. BSSN dengan Kemkominfo bisa saling berkesinambungan untuk bertanggung jawab dan menanggulangi kasus kebocoran data pribadi PDNS2. Tanggung jawab terhadap keamanan siber tetap merupakan tanggung jawab dari BSSN sebagaimana yang dimaksud dalam visi misi atau semangat pembentukan BSSN, akan tetapi BSSN juga harus dibantu dengan Kementerian/Lembaga/Satuan Kerja Perangkat Daerah/Institusi terkait.

DAFTAR PUSTAKA

1. Jurnal

- Ardipandanto, Aryojati “Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber”, *Info Singkat* 16, No. 13 (2024): 7-9
- Ginanjar, Yusep, “Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara”, *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, No.2 (2022): 295-316, <https://doi.org/10.36859/jdg.v7i02.1187>
- Guna, Tedo Hindami, “Breaking down barriers: Overcoming silo mentality in bureaucratic reform” *Journal of Sustainability, Society, and Eco-Welfare* 2, No. 1 (2024): 16–28, <https://doi.org/10.61511/jssew.v2i1.2024.884>
- Hartono, Budi, “Ransomware: Memahami Ancaman Keamanan Digital” *Bincang Sains dan Teknologi (BST)* 2, No. 2 (2023): 55-62, <https://doi.org/10.56741/bst.v2i02.353>
- Kusnadi, Sekaring Ayumeida dan Andy Usmina Wijaya, “Perlindungan Hukum Data Pribadi Sebagai Hak Privasi” *Al-Wasath Jurnal Ilmu Hukum* 5, No. 1 (2024): 19-32, <https://doi.org/10.47776/alwasath.v2i1.127>
- Najiyya, Ana & Stepani Sisca Wulandari, “Eksplorasi Implementasi Kebijakan Pembentukan Computer Security Incident Response Team (Csirt) di Kementerian Perdagangan: Sebuah Studi Kualitatif” *Jurnal Riset Akuntansi Multiparadigma* 10, No. 1 (2023): 50-55. <https://doi.org/10.30743/akuntansi.v10i1.7246>
- Prabaswari, Muhamad Alfikri, Irdam Ahmad, “Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah” *Matra Pembaruan Jurnal Inovasi Kebijakan* 6, No. 1 (2022): 1-13, <https://doi.org/10.21787/mp.6.1.2022.1-13>
- Shidique, Muhammad Rafi & Mansur Juned, “Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)”. *Journal of Social and Political Sciences* 6, No. 4 (2023): 215-224. <https://doi.org/10.31014/aior.1991.06.04.457>
- Sudarmadi, Damar Apri dan Arthus Josias Simon Runturambi, “Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia”, *Jurnal*

Kajian Strategik Ketahanan Nasional 2, No. 2 (2019): 163-183,
<https://doi.org/10.7454/jkskn.v2i2.10028>

2. Internet

Eka Yudha Saputra, “Benarkah BSSN Abai Melindungi Pusat Data Nasional” Terakhir diubah 26 Juni 2024, <https://www.tempo.co/politik/abai-bssn-pusat-data-nasional-410023>

Luthfiani, Desty, “Peretas Pusat Data Nasional Minta Tebusan Rp 131 Miliar” Terakhir diubah 24 Juni 2024. <https://www.tempo.co/politik/peretas-pusat-data-nasional-minta-tebusan-rp-131-miliar-46354>

Yuliansron, “Indonesia Jadi Target Utama Ransomware di Asia Tenggara: Begini Cara Lindungi Data Kamu!” Terakhir diubah 20 Des 2024. <https://www.liputan6.com/tekno/read/5842580/indonesia-jadi-target-utama-ransomware-di-asia-tenggara-begini-cara-lindungi-data-kamu>

3. Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
Undang

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan
Sistem Elektronik

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan
Manajemen Krisis Siber

Peraturan BSSN No. 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara
Tahun 2020-2024