PERLINDUNGAN HUKUM PADA PUSAT DATA NASIONAL TERHADAP KEJAHATAN PERETASAN DATA

(TESIS)

Oleh
CHESSYA TIVANI WIJAYA

PROGRAM STUDI MAGISTER ILMU HUKUM
FAKULTAS HUKUM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2025

ABSTRAK

Pusat Data Nasional Kementerian Komunikasi dan Digital mengalami peretasan data pada tahun 2024 yang menyebabkan kebocoran data, hal ini berdampak pada keamanan data dan informasi publik di Indonesia. Kejadian ini merupakan peringatan bagi pemerintah untuk dapat memitigasi hal serupa agar tidak terjadi dikemudian hari. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap data dan infromasi di Pusat data Nasional serta mengkaji strategi kelembagaan di Indonesia dalam perlindungan data nasional di masa mendatang. Pendekatan yang digunakan dalam penelitian pendekatan peraturan perundang-undangan, guna pendekatan konseptual dan pendekatan kasus.

Peraturan perundang-undangan di Indonesia sudah mengatur mengenai perlindungan data, tercantum pada Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pemerintah sendiri telah mengeluarkan kebijakan terkait perlindungan data di Indoensia yang tertuang pada Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Indonesia serta membentuk Badan Siber dan Sandi Negara sebagai lembaga yang mengoordinasikan kemana siber di Indonesia. Selain dari peraturan perundang-undangan tersebut, peneliti melihat bahwa adanya kelemahan pada fasilitas dan sumber daya manusia, seperti standar keamanan yang belum optimal dan masih ditemukan serangan-serangan siber yang berasal dari luar.

Hasil penelitian menunjukkan bahwa, strategi pemerintah Indonesia dalam perlindungan data nasional untuk membentuk lembaga pengawas yang bertugas untuk mengawasi pengelolaan data dan informasi nasional sesuai dengan yang diamanatkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi salah satu langkah untuk memitigasi dan meminimalisir adanya serangan siber yang masuk ke Indoensia. Maka, diperlukan kolaborasi antar kelembagaan dan diadakannya lembaga pengawas perlindungan data untuk mengisi kelemahan diatas agar pengeloaan keamanan data dapat lebih optimal dan berkelanjutan.

Kata Kunci: Keamanan Siber**,** Peretasan Data, Perlindungan Hukum, Pusat Data Nasional.

ABSTRACT

The Ministry of Communication and Digital's National Data Center experienced a data breach in 2024, resulting in a data leak. This impacted the security of public data and information in Indonesia. This incident served as a warning to the government to mitigate similar incidents to prevent future recurrences. This study aims to analyze the legal protection of data and information at the National Data Center and examine Indonesia's institutional strategies for national data protection in the future. The approach used in this research is a legislative approach, using both a conceptual and case-based approach.

Indonesian laws and regulations already regulate data protection, as outlined in Law Number 1 of 2024 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection. The government has issued policies related to data protection in Indonesia, outlined in Presidential Regulation Number 39 of 2019 concerning One Data Indonesia, and established the National Cyber and Crypto Agency as an agency to coordinate cyber security in Indonesia. In addition to these laws and regulations, researchers observed weaknesses in facilities and human resources, such as suboptimal security standards and the continued presence of cyberattacks originating from abroad.

The research findings indicate that the Indonesian government's national data protection strategy, which involves establishing a supervisory agency tasked with overseeing the management of national data and information, as mandated by Law Number 27 of 2022 concerning Personal Data Protection, is one step in mitigating and minimizing cyberattacks entering Indonesia. Therefore, inter-institutional collaboration and the establishment of a data protection supervisory agency are needed to address these weaknesses, ensuring more optimal and sustainable data security management.

***Keywords**: Cyber Security, Data Hacking, Legal Protection, National Data Center.*

PERLINDUNGAN HUKUM PADA PUSAT DATA NASIONAL TERHADAP KEJAHATAN PERETASAN DATA

Oleh

CHESSYA TIVANI WIJAYA

2322011009

TESIS

Sebagai Salah Satu Syarat Untuk Mencapai Gelar
MAGISTER HUKUM

Pada

Program Studi Magister Ilmu Hukum
Fakultas Hukum Universitas Lampung

PROGRAM STUDI MAGISTER ILMU HUKUM
FAKULTAS HUKUM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2025

Judul Tesis	:	**PERLINDUNGAN HUKUM PADA PUSAT DATA NASIONAL TERHADAP KEJAHATAN PERETASAN DATA**
Nama Mahasiswa	:	Chessya Tivani Wijaya
Nomor Pokok Mahasiswa	:	2322011009
Bagian	:	Hukum Bisnis
Fakultas	:	Hukum

MENYETUJUI
Dosen Pembimbing

Pembimbing I

Dr. Ahmad Zazili, S.H., M.H
NIP 197404132005011001

Pembimbing II

Bayu Sujadmiko, S.H., M.H., Ph. D
NIP 198504292008121001

MENGETAHUI
Koordinator Program Studi Magister Ilmu Hukum
Fakultas Hukum Universitas Lampung

Dr. Heni Siswanto, S.H., M.H.
NIP 196502041990031004

MENGESAHKAN

1. Tim Penguji

Ketua : **Dr. Ahmad Zazili, S.H., M.H.** .....

Sekretaris : **Bayu Sujadmiko, S.H., M.H., Ph. D.** .....

Penguji : **Dr. Sunaryo, S.H., M. Hum.** .....

Penguji : **Rohaini, S.H. M.H., Ph. D.** .....

Penguji : **Prof. Dr. I Gede AB Wiranata, S.H., M.H.** .....

2. Dekan Fakultas Hukum

Dr. M. Fakih, S.H., M. S
NIP 196412181988031002

Tanggal Lulus Ujian Tesis: 3 September 2025

LEMBAR PERNYATAAN

Dengan ini saya menyatakan dengan sebenarnya bahwa:

1. Tesis saya yang berjudul **"Perlindungan Hukum Pada Pusat Data Nasional Terhadap Kejahatan Peretasan Data"** adalah benar hasil karya sendiri dan bukan hasil plagiat atau pengutipan atas karya penulisan lain dengan cara yang tidak sesuai dengan etika ilmiah yang berlaku.
2. Hak intelektual atas karya ilmiah ini diserahkan sepenuhnya kepada Universitas Lampung. Atas pernyataan ini apabila di kemudian hari ternyata ditemukan adanya ketidakbenaran, saya bersedia menanggung akibat dan sanksi yang di berikan kepada saya, maka saya bersedia dan sanggup di tuntut sesuai dengan ketentuan yang berlaku.

Bandar Lampung, 03 September 2025

Penulis,

Chessya Tivani Wijaya
NPM 2322011009

RIWAYAT HIDUP

Penulis bernama lengkap Chessya Tivani Wijaya, dilahirkan di Kotabumi pada tanggal 02 April 2000. Penulis merupakan anak pertama dari dua bersaudara dari pasangan Bapak Hilman Adiwijaya, S.E dan Ibu Riswanti, S.E.

Adapun pendidikan formal yang pernah di tempuh oleh Penulis adalah sebagai berikut:

1. Taman Kanak-Kanak di TK Sari Teladan pada tahun 2006;
2. Sekolah Dasar di SD N 1 Beringin Raya yang di selesaikan pada tahun 2012;
3. Sekolah Menengah Pertama di SMP N 13 Bandar Lampung yang di selesaikan pada tahun 2015;
4. Sekolah Menengah Atas di SMA N 16 Bandar Lampung yang di selesaikan pada tahun 2018;
5. Mahasiswi kelas Internasional Fakultas Syariah Universitas Islam Negeri Raden Intan Lampung pada tahun 2018;
6. Pada tahun 2023, penulis melanjutkan pendidikan jenjang Strata Dua (S2) pada Program Studi Magister Ilmu Hukum Fakultas Hukum Universitas Lampung.

MOTTO

“Seribu terimakasihku untuk orang-orang yang mencintaiku, dan sejuta maafku karena tidak bisa membalasnya”

-Chessya Tivani Wijaya-

PERSEMBAHAN

Dengan teriring doa, rasa syukur, dan segala kerendahan hati. Dengan segala cinta dan kasih sayang ku persembahkan tesis ini kepada:

Papaku tercinta Hilman Adiwijaya, S.E, dan Mamaku tercinta Riswanti, S.E. Kedua orangtua yang selama ini telah mendoakan, mendidik, membimbing dan berkorban dengan setulus hati dan rasa cinta yang luar biasa sehingga saya bisa menjadi seorang yang kuat, semoga kelak dapat terus menjadi anak yang membanggakan kalian. Aamiin yra.

Adikku tercinta, Krisnina Maharani yang senantiasa menemaniku dengan segala suka dan duka serta kasih sayang yang memberiku semangat.

Untuk Almamaterku Tercinta Universitas Lampung, tempatku memperoleh ilmu dan merancang mimpi untuk jalan menuju kesukseskan diriku kedepan.

SANWACANA

Dengan mengucapkan Alhamdulilahirobbil'alamin, Segala puji bagi Allah SubhanahuwaTa'ala, Rabb semesta alam, yang Maha Pengasih lagi Maha Penyanyang. Shalawat serta salam senantiasa terlimpah kepada Baginda Rasullah Muhammad, Sallahu'alaihiwasallah, keluarga, sahabat, dan seluruh pengikutnya yang senantiasa mengikuti jalan petunjuk-Nya. Aamiin. Hanya dengan kehendakNya penulis dapat menyelesaikan penulisan tesis yang berjudul "Perlindungan Hukum Terhadap Peretasan Data di Pusat Data Nasional" yang diajukan untuk memenuhi syarat mencapai gelar Magister Hukum pada Fakultas Hukum Univesitas Lampung.

Penulis menyadari masih banyak terdapat kekurangan dalam penulisan tesis ini serta penulis telah mendapatkan banyak bantuan, bimbingan, dan saran dari berbagai pihak yang sangat berharga bagi penulis dalam menyelesai tesis ini, untuk itu pada kesempatan ini penulis menyampaikan terimakasih yang tak terhingga kepada:

1. Prof. Dr. Ir. Lusmeilia Afriani, D.E.A., I.P.M., selaku Rektor Universitas Lampung.
2. Dr. M. Fakih, S.H., M.S., selaku Dekan Fakultas Hukum Universitas Lampung.
3. Dr. Heni Siswanto, S.H., M.H., selaku Koordinator Program Studi Magister Ilmu Hukum Universitas Lampung.
4. Dr. Ahmad Zazili, S.H., M.H., selaku Dosen Pembimbing I, terima kasih atas waktu yang telah di luangkan untuk bimbingan, saran, masukan, motivasi serta kebaikan hatinya dalam membantu penulis menyelesaikan karya ilmiah ini dan bantuan yang sangat berarti, sehingga tesis ini dapat diselesaikan dengan baik
5. Bayu Sujadmiko, S.H., M.H. Ph.D, selaku Dosen Pembimbing II, terima kasih atas waktu yang telah di luangkan untuk bimbingan, saran, masukan serta kesabaran dalam membimbing penulis menyelesaikan karya ilmiah

dan bantuan yang sangat berarti, sehingga tesis ini dapat diselesaikan dengan baik.

6. Dr. Sunaryo, S.H., M. Hum, selaku Dosen Pembahas I, terimakasih atas kesediannya meluangkan waktu, tenaga dan pikirannya untuk memberikan kritik, pengarahan dan saran dalam proses penyelesaian tesis.
7. Rohaini, S.H., M.H., Ph. D, selaku Dosen Pembahas II, terimakasih atas kesediannya meluangkan waktu, tenaga dan pikirannya untuk memberikan kritik, pengarahan dan saran dalam proses penyelesaian tesis.
8. Dr. Rinaldy Amrullah, S.H., M.H, selaku Pembimbing Akademik yang telah membantu dan membimbing penulis dalam perkuliahan di Fakultas Hukum Universitas Lampung.
9. Seluruh Dosen, Staff Adminitrasi dan karyawan yang bertugas di Program Studi Magister Ilmu Hukum yang selama ini telah memberikan ilmu dan pengalaman yang sangat bermanfaat bagi saya.
10. Papa dan Mama menjadi orangtua yang luar biasa dan tak tergantikan yang selalu memberikan doa, semangat dan dukungan untuk kesuksesan penulis terimakasih atas segala bantuan semoga penulis selalu dapat membuat kalian tersenyum bangga.
11. Adikku tercinta Nina yang selama ini selalu memberikan motivasi, dukungan dan doa sehingga penulis dapat mewujudkan impian keluarga dan menjadi teladan bagi adik tercinta.
12. Keluarga Besarku yang selama ini selalu memberikan dukungan, nasehat, dan motivasi kepada penulis selama menjalankan studi di Fakultas Hukum Universitas Lampung.
13. PT Queen Network Nusantara, terima kasih atas kebaikan dan kemurahan hati Bapak Supriyanto dan Ibu Tresna Fuji Lestari telah mengizinkan Penulis untuk melanjutkan Studi Magister. Terima kasih atas waktu, kesempatan yang sangat luar biasa, dukungan dan motivasi yang diberikan kepada Penulis. Terima kasih untuk Mba Ade, Mba Rara, Mba Kiki, Kak Hashfi, Deo, yang selalu menemani agar tetap waras di dua alam. Terima kasih juga kepada seluruh karyawan QNN atas dukungannya yang menghibur dan memberi solusi atas proses ini. Judul tesis ini terinspirasi

dari kesempatan berharga yang diberikan oleh perusahaan kepada Penulis (Surakarta, Solo).

14. Sahabatku "Cabe Terong dan Malming" yang selalu menemaniku dan tidak meninggalkanku, selalu menemani semua prosesku sejak 2015 hingga aku menyelesaikan studi Magister dan selalu berdiri disampingku seterusnya. Terima kasih atas segala support panjang kalian menemaniku berproses dan menerima semua cerita panjangku *up and down* selama proses ini, *the real* menemani sampai aku cantik. Jangan lupain aku ya guys, sayang banget sama kalian pokoknya.
15. Sahabatku seperjuangan di Pascasarjana Ajeng Gustiara Salsabila,S.H.,M.H., Restika Susanti,S.H.,M.H., terimakasih telah bersedia meluangkan waktu untuk selalu menemani, berbagi cerita, memberikan semangat, motivasi, inspirasi, suka duka dalam menjalani persahabatan dan juga canda tawa selama ini semua akan menjadi hal yang selalu terkenang dan tidak bisa di lupakan dan akan menjadi cerita indah dari perjalanan hidup penulis dan semoga kelak kita sukses bahagia bersama.
16. Sahabatkku "Sri Rahayu Wantika, S.H, Shinta Rahmawati, S. Pd, Desliyona, S.H, Adinda Dwi Prestiwi, S. H, Riska Dianda Fadillah, S.H, Anita Milenia Sari Damanik, S.H, terima kasih banyak atas support kalian yang selalu mendengarkan keluh kesahku selama proses panjang ini. Walaupun prosesnya panjang dan terasa berat, tapi dengan ada kalian terasa ringan.

Semoga Allah SWT membalas jasa dan kebaikan yang telah di berikan kepada Penulis. Penulis menyadari bahwa masih terdapat kekurangan dalam penulisan tesis ini karena keterbatasan dan pengetahuan yang penulis miliki, maka dari itu kritik, saran dan masukan yang membangun dari semua pihak sangat di harapkan untuk pengembangan dan kesempurnaan tesis ini.

Bandar Lampung, 03 September 2025
Penulis,

Chessya Tivani Wijaya

DAFTAR ISI

I. PENDAHULUAN

A. Latar Belakang

Salah satu potensi kejahatan pada perkembangan teknologi informasi juga berkaitan pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Melihat kasus yang baru saja terjadi yaitu kebocoran data Pusat Data Nasional yang diduga diretas oleh kelompok peretas lintas negara sebagai kelompok kejahatan terorganisasi *ransomware*. Serangan *ransomware brainchipper* yang tidak hanya mengganggu layanan publik tetapi juga menimbulkan resiko besar terhadap keamanan data pribadi masyarakat. Langkah preventif dan represif serangan siber yang menjadi prioritas utama dalam menjaga kestabilan sistem informasi dan layanan publik di Indonesia. *Downtime* yang berkepanjangan menyoroti dampak ekonomi dari pelanggaran keamanan siber. Adanya peretasan data tersebut mengakibatkan kebocoran data pribadi, informasi rahasia, gangguan operasional yang menghentikan layanan digital seperti layanan E-KTP, BPJS, perpajakan dan sistem layanan publik, selain itu menimbulkan mudahnya akses pencurian data seperti pemalsuan identitas hingga kerugian finansial.

Dalam pernyataannya pada artikel Serikat Media Siber Indonesia Kepala *Communication and Information System Security Research Center* (CISSReC) Pratama Persadha, bahwa kerentanan pada sistem penonaktifan awal *Windows Defender* menunjukkan potensi kerentanan dalam kerangka keamanan. Kegagalan sistem *XDR SIEM* yang terjadi kemudian menyoroti kurangnya antisipasi negara dalam menangani peretasan data. Jika sistem pemantauan keamanan memiliki konfigurasi yang baik atau mumpuni, dampak kerusakan tersebut bisa saja dikurangi. Penggunaan *malware* yang canggih seperti *Lock Bit* dan *Babuk,* yang menggunakan metode enskripsi cepat dan kompleks menunjukkan tingkat kecanggihan serangan yang tinggi.[1] Hal ini menunjukkan bahwa para penyerang

[1] Ertugrul A,14 Mei 2023, *Is SIEM Really Dead? Does XDR Or Other Technologies Replace SIEM? What Types Of Attacks Does SIEM Detect?*, Https://Www.Linkedin.Com/Pulse/Siem-Really-Dead-Does-Xdr-Other-Technologies-Replace-What-Akbas/ , Dikutip Tangal 12 Oktober 2024.

telah dipersiapkan dengan baik dan memiliki kemampuan teknis yang signifikan. Peningkatan investasi dalam teknologi keamanan siber salah satunya dapat dilakukan dengan memperkuat kerja sama internasional untuk menghadapi ancaman siber yang berkembang pesat pelatihan terhadap sumber daya terkait. Pengamanan akses dan data perlu ditingkatkan mengingat berkenaan dengan kejahatan pada perkembangan teknologi informasi khususnya pengelolaan keamanan data pribadi yang membutuhkan perlindungan. Pentingnya mengenai perlunya sebuah aturan tentang perlindungan data semakin berkembang pemerintah semakin menyadari sangat beresiko hal-hal seperti ini di Indonesia. Mengenai kebijakan yang diterbitkan di Indonesia saat ini justru tidak dapat melindungi salah satu pertahanan negara, apalagi sekarang diperkuat dengan adanya regulasi baru.[2]

Berdasarkan monitoring trafik internet yang dilakukan oleh Badan Siber Dan Sandi Negara pada tahun 2022 terjadi Anomali Trafik sebanyak 976.429.996, dengan aktivitas *Malware APT* sebanyak 4.421.992, *Website Hacking* 2.348, dan laporan insiden siber sejumlah 236. Kemudian pada Anomali Trafik pada tahun 2023 untuk keseluruhan sejumlah 403.990.813 yang dalam catatannya 44,47% atau 179.637.404 merupakan *Malware Activity*, 33,28% atau 134.446.045 merupakan *Trojan Activity*, 9,36% atau 37.809.262 yang merupakan *Information Leak*, sedangkan lainnya 12,89%. Jadi menurut data yang diungkapkan oleh Badan Siber Dan Sandi Negara terdapat tiga jenis anomali yang sering terjadi di Indonesia antara lain 66,27% atau 153.361.447 yang merupakan *Malware Activity*, 17,42% atau 40.315.967.[3]

Data terbaru 2023 jumlah serangan siber meningkat menjadi 97,53% atau 338.599.835. Dan pada tahun 2024 pada semester 1 terjadi sebanyak 619,95% atau 2.152.313.419.[4] Jika melihat dari data-data tersebut diatas jumlah serangan siber di Indonesia terkadang meningkat dan menurun. Inilah yang melatar belakangi bahwa regulasi untuk perlindungan data dan keamanan siber perlu diperhatikan. Melihat ketimpangan ini menandakan bahwa masih banyak lembaga pemerintahan,

[2] Ruben Coda Sifiq Indonesian, Dkk, "Analisis Privasi Data Pengguna Dalam Instansi BPJS Kesehatan", *Prosiding Seminar Sitasi, UPN Veteran Jawa Timur*, 13 November 2021, Hal. 178

[3] Badan Siber Dan Sandi Negara

[4] Awan Pintar, Https://Map.Awanpintar.Id/ , Dikutip Tanggal 19 Februari 2025

perusahaan, bahkan masyarakat yang belum teredukasi atau sepenuhnya patuh terhadap aturan mengenai perlindungan data, termasuk penerapan standar keamanan siber yang masih rendah. Banyak institusi yang belum memiliki sistem keamanan data yang kuat sehingga menjadi target empuk bagi peretas. Regulasi yang ada di Indonesia masih belum terintegrasi dengan standar internasional yang menyebabkan masih adanya celah hukum yang memungkinkan penyalahgunaan data pribadi dari dalam maupun luar negeri. Mengacu pada regulasi internasional yaitu *General Data Protection Regulation* (GDPR), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)[5] dan Undang-Undang Nomor 1 Tahun 2024[6] perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)[7] berperan kompleks untuk melindungi data pribadi di Indonesia mengingat terjadinya kebocoran data yang dialami oleh Pusat Data Nasional yang infrastrukturnya memiliki kelemahan padahal seharusnya memiliki tingkat keamanan yang tinggi karena menyimpan data strategi nasional. Apabila kita melihat sisi normatifnya dalam menghadapi lonjakan dari serangan siber di Indonesia yang dimana perlu mencakup penguatan regulasi, penegakan hukum, serta edukasi ke seluruh stakeholder terkait dengan keamanan siber.

Berangkat dari data tersebut dengan adanya regulasi yang dibuat oleh pemerintah mengharuskan adanya sebuah kepastian atas pengelolaan data dan informasi, sebab tanpa pengolahan data dengan baik dan tepat maka akan berujung pada penyalahgunaan dan serangan kejahatan siber. Yang dalam praktiknya memang masih banyak anomali dari serangan-serangan siber yang menimbulkan banyak kerugian untuk perlindungan data pribadi. Berdasarkan data diatas menunjukkan bahwa adanya lonjakan yang menunjukkan bahwa serangan siber di Indonesia terus meningkat drastis. Seperti kasus peretasan data pribadi pada Pusat Data Nasional yang mengakibatkan 47 layanan Kementerian, Pendidikan,

[5] Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

[6] Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

[7] Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Kebudayaan, Riset, dan Teknologi Republik Indonesia termasuk Kartu Indonesia Pintar, pemadanan Nomor Pokok Wajib Pajak warga asing pada Kementerian Keuangan, gangguan aplikasi Srikandi Pemerintah Solo terganggu, pelayanan imigrasi di bandara, hingga Penerimaan Peserta Didik Baru melalui online di Dumai dibatalkan.[8]

Kini serangan siber di Indonesia bukan lagi sekedar ancaman, tetapi sudah menjadi kenyataan yang bahkan terjadi di Indonesia bila melihat data-data yang dipaparkan di atas hampir setiap hari serangan selalu masuk ke Indonesia, jika tidak dibarengi dengan ketahanan yang kokoh bisa saja kasus seperti peretasan data pribadi yang dialami oleh Pusat Data Nasional kembali terulang. Terkait dengan kejahatan siber bahwa isi dari UU ITE tidak memberikan pengklasifikasian yang eksplisit mengenai kejahatan siber. Serta pengaturan dalam UU ITE tidak mengatur kejahatan tetapi justru menyamakannya dengan tindak pidana konvensional. D.D Machmuddin dan B. Pratama dalam *Some of Indonesia Cyber law Problems* menjelaskan bahwa pembentukan UU ITE terkesan dibuat terlalu awal dan tidak memperhatikan penempatan media akses, dari segi komputer maupun variasinya. Pembahasan ini penting karena dapat memberikan konfirmasi jelas mengenai pencurian data yang tergolong kejahatan siber. Analisis mengenai isi dari Undang-Undang yang dapat diadaptasikan dalam perubahan di bidang teknologi.

Namun memiliki kekurangan karena cenderung menjadi duplikasi dari hukum konvensional, serta sama sekali tidak membahas mengenai perlindungan terhadap jaminan keamanan dan kerahasiaan di ruang siber. Kelemahan UU ITE salah satunya adalah tidak adanya pembahasan mengenai data. Hal ini perlu diperhatikan mengingat potensi bahaya dari *leakage and espionage* (membocorkan data kendala yuridis dan kendala penanganan spionase) serta yang dapat mengancam masyarakat luas yaitu pencurian identitas virtual.[9] Dalam UU ITE tidak menyebutkan sedikitpun tentang kelalaian yang dibuat oleh pengelola situs sehingga *hacker* bisa masuk dengan leluasa. Kegiatan yang lain yang sama pentingnya salah satunya dalam Kitab Undang-Undang Hukum Pidana pada Pasal

[8] Hafidz Mubarak, 29 Juni 2024, Deret Layanan Terdampak Peretasan Pusat Data Nasional, Https://Www.Cnnindonesia.Com/Nasional/20240628202216-12-1115511/Deret-Layanan-Terdampak-Peretasan-Pusat-Data-Nasional , Dikutip Tanggal 29 Juni 2024

[9] Wisnu Handi Prabowo, Satriya Wibawa, Fuad Azmi, "Perlindungan Data Personal Siber Di Indonesia", *Jurnal Relasi Internasional Padjajaran,* Vol. 1 No. 3 Januari 2020, Hlm. 220

53 menerangkan tentang turut serta dalam kejahatan *hacking,* pengaturan mengenai dikenakan sanksi pidana ataupun tidak masih belum jelas pengaturannya.[10]

Mengkaji dari aturan yang berlaku di Indonesia bahwa dalam perlindungan data pribadi telah dipayungi oleh UU PDP dan UU ITE. Namun secara struktural birokrasi yang berwenang dalam pengelolaan perlindungan data pribadi di Indonesia yaitu Kementerian Komunikasi Dan Digital, sedangkan yang paling bertanggung jawab atas perlindungan data pribadi adalah Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika), selain itu sektor lain dalam pengelolaan dan perlindungan data pribadi menjadi tanggung jawab individu. Setiap kementerian memiliki server masing-masing yang tidak sepenuhnya terdeteksi oleh Komunikasi Dan Informasi Digital, maka dari itu diperlukan *back up* data apabila terjadi peretasan seperti yang dialami oleh Pusat Data Nasional. *Back up* data ini memang memakan waktu, padahal *back up* data juga bisa dilakukan secara *real time*. Melihat ada potensi atau celah saat tidak memiliki pertahanan atau bahkan hanya satu lapisan yang rentan, *back up* data pada server terdapat keuntungan bagi pihak yang tidak bertanggung jawab dan bisa saja disalahgunakan sehingga merugikan.

Nyatanya undang-undang tidak juga berhasil melindungi data, berangkat dari hal tersebut pemerintah membentuk Badan Siber dan Sandi Negara yang merupakan bagian dari langkah strategis dalam upaya menjaga kedaulatan ruang siber melalui tata kelola pengamanan yang kuat. 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. 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.[11]

---

[10] Rini Retno Winarni, " Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana *Cyber Crime"* , *Jurnal Hukum Dan Dinamika Masyarakat* Vol.14, No.1 Oktober 2016, Hlm. 25

[11] M. Prakoso Aji, "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)", *Jurnal Politica,* Vol. 13 No. 2 Nov 2022, Hlm. 228

Dalam pernyataannya Menteri Komunikasi dan Informatika Johnny G. Plate mengatakan bahwa langkah yang diambil oleh Indonesia dalam menanggulangi kebocoran data melalui literasi digital jangka Panjang dan jangka pendek serta mempunyai sistem, model dan pilihan teknologi enkripsi yang kuat. Penyelenggaraan Sistem dan Transaksi Elektronik juga menjadi tata kelola sebagai perpanjangan tangan dari masyarakat yang memiliki data atau pengolah data. Kementerian Informasi dan Digital sebagai regulator mengidentifikasi sedari dini letak terjadinya kebocoran data.[12] Sektor perlindungan data dan keamanan sebagai pondasi awal menyusun kedaulatan negara terkait data dan informasi. Pengembangan kapabilitas sumber daya dan fasilitas akan membuat pertahan tersebut menjadi kokoh. Perlindungan data dalam teori *self determination* sangat memerlukan regulasi yang mewadahinya. Seiring dengan pertumbuhan teknologi, ancaman siber terus mengalami peningkatan yang sangat pesat. Untuk menjaga stabilitas keamanan maka dibutuhkan suatu modifikasi agar pengelolaan jaringan berjalan dengan baik.

Pada Rancangan Anggaran Pendapatan dan Belanja Negara tahun 2023, anggaran diberikan untuk Badan Siber dan Sandi Negara yang merupakan lembaga khusus untuk menangani keamanan siber sebesar Rp 624 Miliar, sedangkan Kepala Badan Siber dan Sandi Negara menyebutkan bahwa anggaran dibawah Rp1 triliun tergolong kurang untuk merealisasikan pertahanan siber.[13] Sedangkan anggaran belanja keamanan siber di tahun 2024 sebesar Rp 303,34 Miliar dan untuk Badan Siber dan Sandi Negara Rp 771,7 Miliar jumlah ini meningkat 21% dibandingkan tahun 2023. Kemudian untuk pagu alokasi tahun anggaran 2025 anggaran belanja Badan Siber dan Sandi Negara sebesar Rp 1.321.636.821.000 yang disetujui oleh Komisi I DPR RI.[14]

---

[12] Wahyu Sudoyo, 1 Juni 2022, ***Ini Langkah Indonesia Cegah Kebocoran Data***, Https://Infopublik.Id/Kategori/Nasional-Sosial-Budaya/636619/Ini-Langkah-Indonesia-Cegah-Kebocoran-Data

[13] Ardimansyah, Dkk, "Tantangan Penanganan Ancaman Siber Dalam Menyongsong Pemilihan Umum 2024", *Jurnal Budget Issue Brief*, Vol. 02, 16 September 2022, Hlm. 2

[14] Chella Defa Anjelina, Mahardini Nur Afifah, 01 Januari 2024, Menkominfo Sebut Anggaran BSSN Terbatas, Benarkah? Ini Besarnya 5 Tahun Terakhir, Https://Www.Kompas.Com/Tren/Read/2024/07/01/150000265/Menkominfo-Sebut-Anggaran-Bssn-Terbatas-Benarkah-Ini-Besarnya-5-Tahun?Page=All , Dikutip Tanggal 12 Februari 2025

Selain itu Pusat Data Nasional mengadakan belanja infrastruktur melalui Kementerian Komunikasi dan Digital yang digunakan untuk operasional dan pemeliharaan BTS 4G senilai Rp1,6 triliun, dengan kapasitas satelit Rp 700 miliar, dan Palapa Ring Rp1,1 triliun. Sri Mulyani mengatakan, belanja untuk Kementerian Informasi Dan Digital cukup besar, mendekati Rp5 triliun. Dan anggaran yang baru saja keluar untuk mengembalikan data Pusat Data Nasional yang diretas oleh pengirim ransomware senilai 8 juta dolar AS atau Rp 131 miliar hanya untuk membuka data.[15] Pada 17 Mei 2023 Kejaksaan Agung menetapkan Johnny G Plate Menteri Komunikasi dan Informatika sebagai tersangka korupsi mega proyek pembangunan menara *Base Transceiver Station* (BTS) sebuah program kerja dari Kementerian Kementerian Komunikasi dan Digital untuk membangun sebanyak 7.904 *Base Transceiver Station* (BTS) 4G di wilayah Terdepan, Terluar, dan Tertinggal (3T). Mega Proyek *Base Transceiver Station* (BTS) 4G tersebut pada awalnya diberi dana sekitar Rp 28 triliun. Pada tahun 2020, telah dicairkan dana sebesar Rp10 triliun dari total Rp 28 triliun untuk membangun 4.200 menara. Kemudian, ditemukan fakta dari pada bulan Mei 2023 bahwa pada bulan Maret tahun 2022, menara yang didirikan hanya sebanyak 958 menara. Dana yang dikeluarkan untuk membangun 958 menara tersebut adalah sebesar Rp2,1 triliun, dan sekitar Rp8 triliun sisa dana untuk membangun 4.200 menara tersebut telah raib di korupsi.[16]

Semestinya anggaran tersebut digunakan sebagai kedudukannya tetapi dianggarkan untuk hal lain. Hal seperti ini yang sering terjadi di Indonesia, dimana sebuah regulasi atau kebijakan yang sudah mendukung tetapi tidak dibarengi dengan sumber daya manusia dan fasilitas yang mendukung. Kebocoran data sering terjadi karena kurangnya antisipasi atau pencegahan dini dari Kementerian Komunikasi Dan Digital sebagai lembaga yang bertanggung jawab dalam pengelolaan data dan Badan Siber Dan Sandi Negara sebagai lembaga yang

---

[15] Dina Karina, ***Pusat Data Nasional Belanjakan Anggaran Rp 700 M Sepanjang 2024, Tapi Kini Terkena Serangan Siber***, Https://Www.Kompas.Tv/Ekonomi/518371/Pusat-Data-Nasional-Belanjakan-Anggaran-Rp700-M-Sepanjang-2024-Tapi-Kini-Terkena-Serangan-Siber?Page=All , Dikutip Tanggal 27 Juni 2024.

[16] Althafferani F Nasution, Dkk, "Pengaruh Tindak Pidana Korupsi Mega Proyek BTS *(Base Transceiver Station)* Oleh Kementerian Komunikasi dan Digital Terhadap Tingkat Kepercayaan Mahasiswa Ilmu Politik UPN Veteran Jakarta", *Jurnal Independen,* Vol.5, No.1, April 2024, Hlm. 14

mendukung Kementerian Komunikasi Dan Digital dalam keamanan siber. Namun, terkait Rancangan Undang-Undang 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. 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. Saat ini UU PDP sudah disahkan, publik dan masih menunggu implementasi dari regulasi ini kedepannya. 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.

Pasal 2 dalam 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 berkaitan dengan kepentingan Indonesia, kepentingan memberikan keamanan data, dan kepentingan strategis lainnya, namun juga termasuk kedaulatan negara. Ancaman hukuman dapat dikenakan pada perbuatan yang dilarang jika seseorang melakukan pelanggaran terhadap Pasal 27 hingga Pasal 34 UU ITE melakukan pembobolan tanpa izin yang tertuang eksplisit sebagaimana dimaksud Pasal 36 UU ITE yang dijalankan di luar area Indonesia terhadap sistem elektronik yang ada di Indonesia.[17]

Dalam Hukum Internasional hanya berlaku konvensi internasional, itupun belum berlaku aktif. Saat ini hanya terbentuk draft *United Nation Cybercrime* yang akan diberlakukan untuk menangani peretasan internasional. Adapun *Budapest Convention* yang berlaku di Uni Eropa, GDPR *(General Data Protection Regulation)* yang berlaku di Uni Eropa. Konvensi tersebut menjadi salah satu acuan untuk penanganan peretasan data internasional dan kerjasama internasional

[17] *Ibid,* Hlm. 232

terhadap perlindungan data. Dalam menangani peretasan data nasional juga memerlukan koordinasi dan dukungan dari kekuatan nasional itu sendiri. Kementerian Komunikasi dan Digital dan Badan Siber Dan Sandi Negara ikut memiliki peran penting dalam menjaga keamanan siber di ruang data, namun kemampuan kedua lembaga ini dalam mencegah peretasan sepenuhnya bergantung pada beberapa faktor. Jika undang-undang sebagai landasan hukum yang implementasinya bergantung pada tindakan yang konkret maka bisa didukung juga dengan infrastruktur teknologi serta sumber daya manusia yang memang ahli dalam bidangnya.

Secara normatif di Indonesia telah memiliki beberapa regulasi yang seharusnya mampu memberikan perlindungan terhadap data pribadi, data informasi, serta antisipasi dalam menghadapi kebocoran data atau kejahatan siber, di antaranya:

1. UU ITE[18] diamanatkan mengatur aktivitas elektronik, menjamin hukum dalam transaksi elektronik, serta memberi dasar hukum untuk menindak kejahatan siber. Seperti yang tercantum Pasal 30 UU ITE bahwa, melarang setiap orang mengakses komputer atau sistem elektronik milik orang lain tanpa hak, termasuk upaya peretasan. Kemudian Pasal 46 dan Pasal 48, dan 51 UU ITE yang mengatur sanksi pidana bagi pelanggaran pasal-pasal seperti peretasan, manipulasi, maupun penyalahgunaan data. Pada Pasal 40 dan Pasal 41 UU ITE disebutkan bahwa memberikan kewenangan kepada pemerintah utnuk emlindungi kepentingan umum dari segala gangguan penyalahgunaan informasi elektronik, termasuk keamanan data startegis.[19]

Secara preventif UU ITE mengatur standar keamanan sistem yang harus dipenuhi oleh Pusat Data Nasional, yang mengacu pada regulasi keamann data untuk mencegah kebocoran data. Sedangkan secara represif UU ITE memberikan dasar hukum bagi yang lalai atau menyalahgunakan akses ilegal hingga sanksi pidana dan denda sebagai bentuk perlindungan hukum. Kebocoran data nasional juga dipengaruhi oleh lemahnya regulasi dan penegakan hukum di bidang keamanan siber. UU ITE dan regulasi turunannya dinilai belum cukup spesifik dalam

[18] Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

mengatur standar teknis keamanan data, seperti penggunaan enkripsi, audit keamanan, dan kewajiban pelaporan insiden.[20]

2. UU PDP[21] yang bertujuan memberikan perlindungan atas hak privasi setiap individu, mengatur pengumpulan, pengolahan, penyimpanan, dan penghapusan data pribadi secara legal dan aman. Regulasi ini secara komprehensif mengatur hak subjek data, kewajiban pengendali atau pemroses data, serta sanksi jika terjadinya pelanggaran data. Peraturan ini pada Pasal 4 dan Pasal 5 UU PDP mengatur bahwa hak subjek data pribadi, seperti hak atas kerahasiaan, hak mengakses, dan hak mendapatkan informasi terkait pemrosesan data, apabila terjadinya suatu kebocoran data maka terjadilah pelanggaran terhadap hak-hak tersebut. Tertulis pada Pasal 20 dan Pasal 22 bahwa kewajiban dari pengendali data pribadi untuk melindungi dan memastikan keamanan data, serta tanggung jawab atas pengelolaan data sedangkan Pusat Data Nasional termasuk pengendali data publik.

Sanksi terkait dengan kebocoran data tercantum pada Pasal 67 hingga Pasal 70 sanksi pidana bagi pihak yang secara melawan hukum mengungkapkan, meperoleh, atau menggunakan data pribadi orang lain.[22] Secara preventif UU PDP mengatur tata kelola data di Pusat Data Nasional mulai dari legalitas, keamanan teknis, hingga standar operasional prosedur penanganan insiden. Undang-undang ini mendorong perlunya penerapan *Data Protection Impact Assesment* sebelum dat diproses hingga memastikan *check and balance* melalui laporan dan audit. Jika terjadi kebocoran data UU PDP mengedepankan transparansi, penegakan sanksi administratif terhadap pengelola data dan pidanan bagi pihak yang sengaja membocorkan data.

UU PDP juga mendukung keberadaan lembaga pengawas perlindungan data pribadi sehingga menjamin adanya pihak independen yang mengawasi Pusat Data Nasional. Perlindungan data pribadi dalam konteks digital diatur dalam UndangUndang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, yang

[20] Imanuel Toding Bua, "Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional Tahun 2024, *Jurnal Desentralisasi*, Vol. 2, Nomor 2, Mei 2025, hlm. 106

[21] Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

juga memperjelas bahwa perlindungan data pribadi merupakan komponen dari hak asasi manusia dan menetapkan kewajiban bagi pengelola data untuk menjaga keamanan dan kerahasiaan data yang mereka kelola. UU PDP mengharuskan pengelola data untuk mengikuti tahapan-tahapan keamanan yang sesuai untuk melindungi informasi data pribadi yang dikelola.[23]

3. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres Satu Data Indonesia)[24] bertujuan mewujudkan data yang terpadu, akurat, dan dapat dipertanggungjawabkan, serta mendukung perencanaan, pelaksanaan dan evaluasi, dan pengendalian pembangunan secara efektif dan efisien di seluruh Indonesia. Tertulis pada Pasal 2 kebijakan satu data indonesia yang menekankan pada standarisasi data untuk mendukung perencanaan, pelaksanaan, evaluasi, dan pengendalian data. Namun, semakin banyak terintegrasinya data di Pusat Data Nasional justru semakin meningkatkan risiko kebocoran data, baik yang privat maupun data strategis. Pasal 28 dan Pasal 29 juga mewajibkan adanya mekanisme koordinasi dan pengawasan dalan pengelolaan data termasuk aspek keamanan.[25]

Peraturan presiden ini secara preventif menetapkan standar data untuk meminimalisir pengeloaan data yang bisa menimbulkan celah keamanan data. Dengan adanya walidata dalam peraturan presiden ini membuat koordinasi yang lebih jelas, sehingga tanggung jawab keamanan data lebih terstruktur. Walaupun peraturan presiden ini tidak mengatur sanksi pidana atau administratif atas kebocoran data, peraturan presiden ini memberi kerangka tata kelola yang menjadi pondasi perventif bagi perlindungan hukum.

Dengan adanya satu data Indonesia ini diharapkan data yang dihasilkan merupakan data yang memiliki integritas tinggi yang dimutakhirkan, dan dapat diakses luas oleh masyarakat dengan mudah yang dapat digunakan kembali atau dipakai oleh pengguna data. Merujuk pada tujuan pembuatan kebijakan Satu Data Indonesia yang tertuang dalam Perpres Satu Data Indonesia ditujukan untuk mewujudkan

[23] Muhammad Asthi Seta Ari Yuwana, "Analisa Dampak Kebocoran Data Pusat Data Nasional Dalam Perspektif HAM", *Jurnal Wicarana*, Vol. 4, Nomor 1, Maret 2025, hlm. 34

[24] Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112

ketersediaan data secara akurat, mutakhir, terpadu, dapat dipertanggungjawabkan, aksesibel, serta dapat dibagi pakaikan dan diperbaharui oleh tiap-tiap instansi pemerintah, guna mendukung perencanaan, pemantauan, evaluasi, dan pengendalian pembangunan.[26]

Secara ideal, regulasi serta kebijakan ini dapat memberikan pengamanan sistem informasi yang ketat, penegakan hukum yang jelas terhadap pelaku kejahatan siber, mengatur tanggung jawab penyelenggara sistem elektronik atas insiden kebocoran data, hingga edukasi dan kesiapsiagaan seluruh stakeholder terhadap serangan siber. Namun pada kenyataanya implementasi dari regulasi serta kebijakan tersebut masih perlu di evaluasi dan dimatangkan. Kebocoran data yang dialami oleh pusat data nasional mencerminkan adanya kelemahan pada beberapa aspek utama infrastruktur dan manajemen keamanan siber. Pasca insiden kebocoran data yang muncul soratan bahwa koordinasi dan pengawasan antar Lembaga belum optimal, terutama dalam sistem pengamanan dan manajemen risiko. Menurut undang-undang informasi dan transaksi elektronik kementerian komunikasi dan digital sebagai penyelenggara utama pusat data nasional yang bertanggung jawab membangun serta mengelola, kemudian didukung oleh badan siber dan sandi negara berdasarkan UU PDP.

Saat ini belum ada Lembaga pengawas independen secara eksplisit yang tercantum sesuai yang diamanatkan UU PDP secara operasional, sehingga tidak ada satu badan yang memiliki yurisdiksi penuh dalam investigasi insiden atas pelanggaran data pribadi di pusat data nasional. Tumpang tindih yurisdiksi dalam perlindungan siber yang di aman pusat data nasional masih dalam pengawasan keamanan oleh badan siber dan sandi negara, sementara pengaturan privasi dan otorisasi penggunaan/pengelola data berada di bawah Kementerian Komunikasi dan Digital dan pemilik data, hal ini dirasa perlu diperjelas dan disinkronisasikan agar selaras pada struktur. Secara hukum dan administratif kebocoran data di pusat data nasional berada pada pihak yang mengelola dan mengendalikan sistem pada pusat data nasional dan saat ini memang merupakan tanggung jawab dari

[26] Bayu Adinegoro, "Kebijakan Satu Data Indonesia: Sebuah Antitesis Semangat Keterbukaan Dan Informasi Publik", *Jurnal Kebijakan,* Vol. 16, Nomor 1, Januari 2025, hlm. 3

kementerian komunikasi dan digital, namun dengan adanya badan siber dan sandi negara pun turut mengambil peran dalam pengawasan tersebut. Sedangkan saat ini di Indonesia sendiri tidak ada ketentuan yang pasti siapa yang bertanggung jawab langsung terhadap pusat data nasional. Karena sejauh ini belum jelas siapa yang benar-benar bertanggung jawab dalam pengawasan dan pengelolaan kedaulatan data selain kementerian komunikasi dan digital.

UU PDP belum secara tegas mengatur mengenai tanggung jawab negara atau instansi pemerintah dalam kebocoran data publik. Masih sering terjadinya lempar-lemparan tanggung jawab antara kementerian komunikasi dan digital dengan badan siber dan sandi negara. Dengan demikian menyoroti menjadi lemahnya pengawasan lintas Lembaga, tidak ada sistem kewenangan yang mengaudit sistem pusat data nasional secara berkala yang menciptakan tidak ada akuntabilitas yang cukup untuk menjamin keamanan sistem. Meskipun Indonesia memiliki regulasi dalam perlindungan data, tetapi masih secara nyata kelemahan dari implementasi kebijakan tersebut. Perlu adanya pembaharuan hukum mengenai penyusunan standar operasional keamanan data yang mengikat, dan kepastian dalam lembaga atau instansi pengawas dalam pengelolaan data untuk memastikan bahwa pengelolaan keamanan data di Indonesia berada pada jalur perlindungan yang kuat dan tepat. GDPR yang merupakan regulasi di Uni Eropa untuk melindungi data pribadi warganya dari penyalahgunaan data. Semua anggota Uni Eropa wajib membentuk instansi yang menjalankan urusan mengenai perlindungan data atau petugas perlindungan data yang disebut dengan *Data Protection Officer* atau disebut juga DPA. DPA merupakan lembaga pemerintah independen yang melakukan supervisi terhadap implementasi peraturan yang mengatur mengenai perlindungan data pribadi dan dibentuk untuk mendindaklanjuti keluhan terhadap pelanggaran data GDPR.[27]

Melihat Pasal 15 ayat (1) UU ITE bahwa, setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik. Dari Pasal tersebut

[27] Syafira Agata Ramadhani, "Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa", *Jurnal Hukum Lex Generalis*, Vol. 3, No. 1, Januari 2022, hlm. 80

menandakan bahwa pusat data nasional yang dikelola oleh Kementerian Komunikasi dan Digital wajib menjamin keamanan sistem elektronik yang digunakan untuk mencegah kebocoran data. Kemudian pada Pasal 58 ayat (2) UU PDP bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh Lembaga, ini yang menjadi dasar bahwa perlu adanya Lembaga pengawas yang bertanggung jawab sebagai pengawas pusat data nasional.

Seperti yang ada pada kasus kebocoran data di pusat data nasional hal ini menunjukkan lemahnya pengawasan, response teknis, serta kurangnya kesiapan infrastruktur digital pemerintah. Mendukung dari regulasi tersebut Presiden menerbitkan Perpres Satu Data Indonesia sebagai pendukung regulasi yang ada terkait dengan perlindungan data. Perlunya penegasan tanggung jawab hukum pada setiap pelaku dalam struktur satu data Indonesia jika terjadi insiden kebocoran data akibat kelalaian atau pelanggaran standar operasional maka melibatkan pelanggaran terhadap undang undang lain seperti perlindungan data pribadi. Semua aktivitas pengolahan data harus terdokumentasi dan dapat diaudit secara berkala. Maka dari itu perlunya di perjelas dan restrukturisasi secara eksplisit yang berwenang bertanggung jawab apabila ditemukan insiden sebagai pencegahan terjadinya serangan insiden kebocoran data.

B. Masalah Dan Ruang Lingkup

Berdasarkan latar belakang yang telah diuraikan maka permasalahan dalam penelitian ini adalah:

1. Bagaimanakah perlindungan hukum terhadap peretasan data dan informasi pusat data nasional?
2. Bagaimanakah strategi lembaga di Indonesia dalam perlindungan data nasional di masa mendatang?

Ruang lingkup penelitian ini meliputi kebijakan dan regulasi terhadap perlindungan data dan informasi di pusat data nasional serta melihat strategi atau langkah yang telah Kementerian Komunikasi Dan Digital dan Badan Siber Dan Sandi Negara lakukan untuk melindungi data nasional dari peretasan data.

C. Tujuan Dan Kegunaan Penelitian

1. Tujuan Penelitian

a. Untuk menganalisis, memahami, dan mengkaji peraturan perundang-undangan yang ada terkait dengan perlindungan hukum terhadap peretasan data dan informasi di Pusat Data Nasional.
b. Untuk mengetahui strategi yang dilakukan oleh Kementerian Komunikasi dan Digital serta Badan Siber dan Sandi Negara dalam mengatur penanganan insiden kebocoran data dari sisi kebijakan hukum terhadap peretasan data di Pusat Data Nasional di tengah regulasi yang sudah ada.

2. Kegunaan Penelitian

a. Secara Teoritis

Secara teoritis untuk menambah wawasan dan ilmu pengetahuan serta bacaan, khususnya bagi penulis dan umumnya bagi pembaca terkait dengan Perlindungan Hukum Terhadap Peretasan Data Di Pusat Data Nasional.

b. Secara Praktis

Secara praktis hasil penelitian ini diharapkan dapat berguna sebagai bahan referensi bagi penegak hukum di Indonesia, juga para peneliti hukum yang penelitiannya terkait dengan tesis ini, khususnya pada perlindungan hukum terhadap keamanan data dan informasi serta perlindungan data nasional.

D. Kerangka Pemikiran

1. Kerangka Teoritik

a. Teori Perlindungan Hukum

Menggunakan teori perlindungan hukum yang dicetuskan oleh Philipus M. Hadjohn bahwa, Perlindungan hukum dapat dibedakan menjadi dua macam yaitu:

a) Perlindungan Hukum Preventif Perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban.

b) Perlindungan Hukum Represif hukum represif merupakan suatu perlindungan akhir berupa sanksi berupa denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran.[28] Philipus M Hadjon dalam bukunya menyebutkan sarana perlindungan hukum ada dua macam, yaitu sebagai berikut:

1. Sarana Perlindungan Hukum Preventif

Perlindungan Hukum Data Pribadi Perlindungan hukum preventif ini, subyek hukum diberikan kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Tujuannya adalah untuk mencegah terjadinya sengketa. Perlindungan hukum preventif sangat besar artinya bagi tindakan pemerintah yang didasarkan pada kebebasan bertindak. Dengan adanya perlindungan hukum preventif pemerintah terdorong untuk bersikap hati-hati dalam mengambil suatu keputusan yang didasarkan pada diskresi. Belum banyak diatur mengenai sarana

[28] Anna S. Wahongan, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Ynag Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2026 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik", *Jurnal Lex Privatum,* Vol. 10, Nomor 1, Januari 2022, hlm. 90

perlindungan huku bagi rakyat yang sifatnya preventif, tetapi dalam perlindungan hukum preventif ini dapat kita temui bentuk sarana preventif berupa keberatan.

2. Sarana Perlindungan Hukum Represif

Perlindungan hukum represif bertujuan untuk menyelesaikan sengketa. Penanganan perlindungan hukum represif ini dilakukan oleh Pengadilan Umum dan Pengadilan Administrasi. Prinsip perlindungan hukum terhadap tindakan pemeritah bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hakhak asasi manusia karena menurut sejarah dari barat, lahirnya konsep-konsep tentang pengakuan dan perlindungan. Sedangkan prinsip yang kedua mendasari perlindungan hukum terhadap tindak pemerintah adalah prinsip negara hukum. Dikaitkan dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia mendapat tempat utama dan dapat dikaitkan dari tujuan negara hukum.[29]

b. Teori Kedaulatan

Pada teori ini Plato mengatakan bahwa kekuasaan bukan bersumber dari pangkat, kekuasaan, kedudukan, atau kekayaan, sedangkan Aristoteles melengkapinya dengan pernyataan sumber kekuasaan negara atau kedaulatan adalah hukum negara itu sendiri. Atas dasar teori di atas diturunkan beberapa teori yang mendasarkan pada bagian utama dalam penegakan kedaulatan tersebut, yaitu kedaulatan Tuhan, kedaulatan raja, kedaulatan negara, kedaulatan rakyat dan kedaulatan hukum. Kedaulatan digital harus dinyatakan aspek regulasi sebagai instrumen pemerintahan. Menjaga kedaulatan digital atau kedaulatan ruang siber adalah bagian dari menjaga kedaulatan bangsa dan keutuhan NKRI. Dengan demikian, kesadaran dan partisipasi masyarakat juga memegang peran penting dalam

[29] Dhoni Martien, "Perlindungan Hukum Data Pribadi", Makassar: Mitra Ilmu, 2023, hlm. 27

kedaualatan digital dan keamanan informasi dari setiap ancaman yang dapat mengganggu tujuan dan kepentingan nasional.

UU PDP yang memberikan hak subjek data, kewajiban pengendali data, serta sanksi pidanan atau administratif. Berdasarkan teori ini negara memiliki legitimasi penuh untuk membuat regulasi yang ada sebagai bentuk perlindungn hukum. Apabila terjadinya kebocoran data dan tanpa perlindungan yang memadai maka terjadilah kegagalan negara dalam menjalankan kedaulatannya. Meningkatkan dari sisi sistem dan teknologi masih dijumpai pusat data dari aplikasi yang digunakan oleh pemerintah dan rakyat Indonesia tidak dapat memiliki kekuatan hukum untuk dapat menjamin datanya aman dan tidak disalahgunakan. Hal inilah yang menjadi kendala utama dalam konteks kedaulatan data. Strategi kebijakan menjaga kedaulatan data dengan memperhatikan regulasi yang memadai, peningkatana kesadaran masyarakat tentang pentingnya kedaulatan data dan partisipasi aktif stakeholder dalam proses pengambilan kebijakan, serta penggunaan sistem dan teknologi yang tepat akan menjadi dasar penting dalam menjaga kedaulatan data nasional.[30]

c. Asas Kehati-Hatian

Asas kehati-hatian dalam konteks perlindungan data pribadi mengacu pada tindakan proaktif dan pencegahan yang diambil oleh pemerintah untuk memastikan bahwa data pribadi dikelola dan dilindungi dengan cara yang aman dan sesuai dengan peraturan perundang undangan yang ada. Hal ini mencakup berbagai tindakan preventif untuk mencegah pelanggaran data dan meminimalkan risiko penyalahgunaan data pribadi. Dalam UU PDP menetapkan adanya otoritas perlindungan data yang bertugas mengawasi kepatuhan terhadap undang-undang tersebut. Pemerintah dan lembaga terkait harus aktif melakukan edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi. Oleh karena itu, seluruh stakeholder,

[30] Taufiq A. Gani, "Menegakkan Kedaulatan Data Digital Dalam Rangka Menjaga Integritas NKRI", Lembaga Ketahanan Nasional Republik Indonesia, http://lib.lemhannas.go.id/public/media/catalog/0010-112300000000102/swf/7439/PPRA%2065%20-%2090%20S.pdf , hlm. 27

perlu mendapatkan pelatihan yang memadai tentang asas kehati-hatian dan praktik terbaik dalam pengelolaan data pribadi.

Sehingga Indonesia perlu mengadopsi standar internasional dalam perlindungan data pribadi untuk memastikan bahwa perlindungan data di Indonesia sejajar dengan praktik terbaik global. Karena dengan adanya kerjasama dengan negara lain dalam berbagi informasi dan teknologi terkait keamanan data dapat membantu meningkatkan perlindungan data pribadi di Indonesia sehingga kejadian peretasan yang yang baru-baru ini tidak terjadi. UU PDP telah mengatur bahwa perlindungan data pribadi seseorang dilaksanakan melalui beberapa asas, salah satunya yaitu asas kehati-hatian, asas kehati-hatian ini menjelaskan bahwa para pihak yang terkait dengan pemrosesan dan pengawasan data pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian.[31]

2. Kerangka Konsep

Kerangka konsep adalah suatu kerangka yang menggambarkan antara konsepkonsep khusus yang merupakan arti-arti yang berkaitan dengan istilah yang digunakan dalam penulisan atau penelitian. Dalam penelitian ini akan dijelaskan mengenai pengertian pokok-pokok istilah yang akan digunakan sehubungan dengan objek dan ruang lingkup penulisan sehingga mempunyai batasan yang jelas dan tepat dalam penggunaannya.

Pusat Data Nasional dirancang sebagai tempat penyimpanan dan pengelolaan data negara yang aman, sehingga memiliki fungsi strategis sebagai penjamin kerahasiaan dan integritas data pribadi maupun data publik. Perlindungan data di Indonesia memiliki dasar hukum yang jelas, antara lain UU PDP, UU ITE, serta Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia dan peraturan terkait lainnya. Namun, untuk mengoperasionalkan perlindungan hukum tersebut tidak cukup hanya dengan regulasi, melainkan juga membutuhkan fasilitas teknologi yang canggih, infrastruktur keamanan

[31] Siti Yuniarti, Erni Herawati, "Analisis Hukum Kedaulatan Digital Indonesia", *Jurnal Pandecta,* Vol.15, No.2, Desember 2020, Hlm. 161

siber yang mutakhir, serta sumber daya manusia yang andal dalam mendeteksi, mencegah, dan merespons serangan peretasan data. Sisi struktur hukum secara kerangka regulasi harus konsisten dan jelas dari struktur kewenangan sehingga tidak menimbulkan tumpang tindih antar lembaga. Diperlukan kesadaran kolektif bahwa keamanan data adalah tanggung jawab bersama, bukan sekadar kewajiban formal atau pemerintah saja melainkan seluruh stakeholder pengelola data. Mekanisme sanksi tegas bagi pelaku peretasan maupun pihak yang lalai wajib diterapkan, disertai penguatan kapasitas aparat penegak hukum dalam menghadapi kejahatan siber. Pada akhirnya, perlindungan data di Pusat Data Nasional menuntut adanya konsep *collaborative governance*, yaitu kolaborasi antara pemerintah/regulator, sektor swasta, masyarakat, dan lembaga perlindungan data independen untuk terciptanya sistem keamanan yang akuntabel, dan mampu menjaga kepercayaan publik terhadap pengelolaan data nasional.

Praktik untuk melindungi sistem, jaringan, dan program dari serangan digital. Serangan-serangan ini biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif; memeras uang dari pengguna; atau mengganggu proses bisnis normal.[32] Maka dari itu Pusat Data Nasionalndibentuk sebagai fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan, pengolahan, dan pemulihan data bagi Instansi Pusat dan Pemerintah Daerah. Penyediaan Pusat Data nasional ditujukan untuk memberikan kemudahan bagi Instansi Pusat dan Pemerintah Daerah untuk mendapatkan layanan Pusat Data dan meningkatkan efisiensi biaya melalui pemanfaatan bersama Pusat Data nasional oleh Instansi Pusat dan Pemerintah Daerah.[33] Dalam sebuah sistem elektronik dalam UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal. Sistem elektronik sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan,

[32] https://www.its.ac.id/it/id/keamanan-siber/

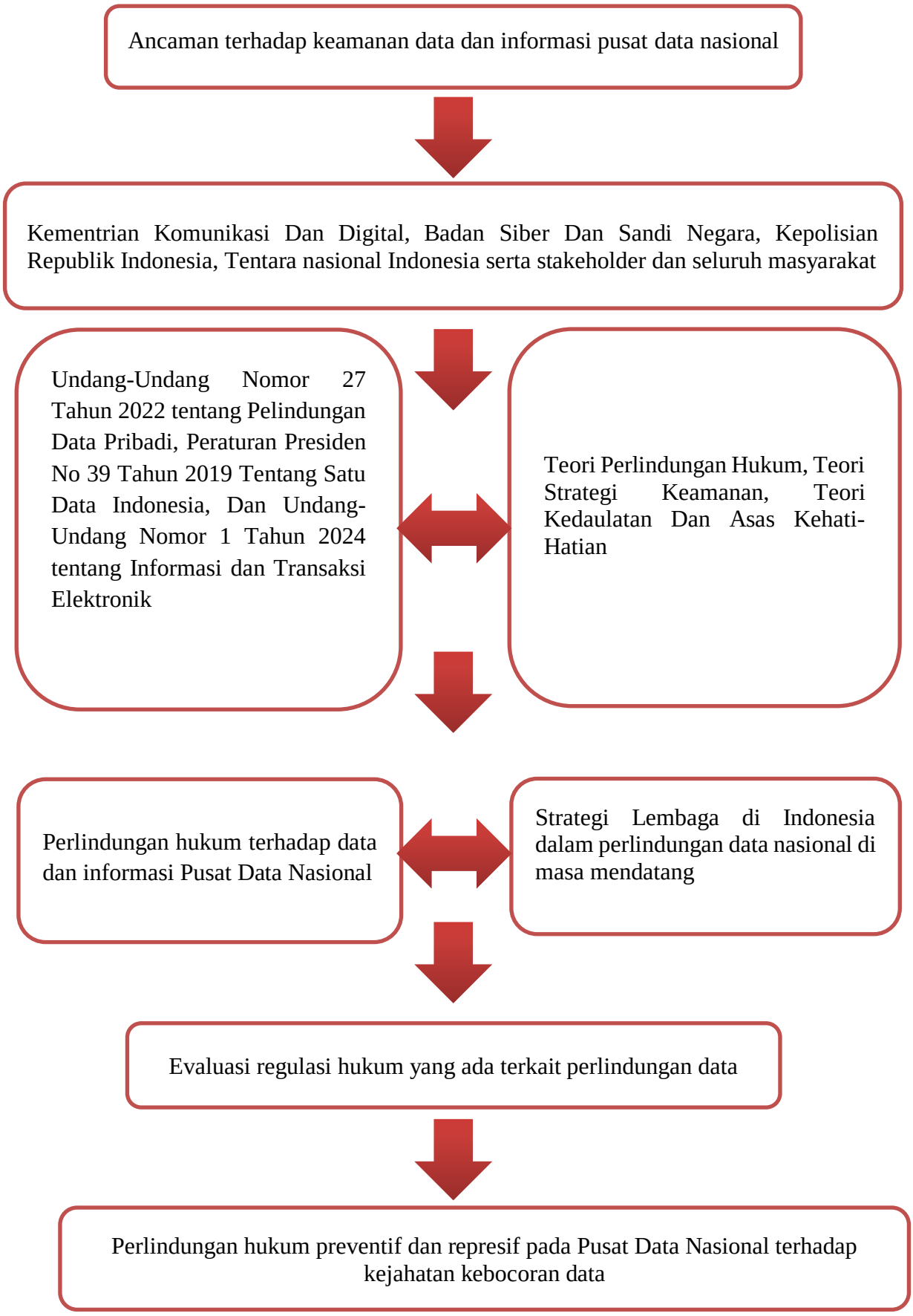
[33]https://www.beltim.go.id/storage/MateriSPBE//CMFXBqEkKnUuhdKfJEMQ4DXsL2I5XPN0iDyD0DJF.pdf

mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Jadi yang termasuk ke dalam sistem elektronik adalah jaringan internet, layanan e-banking, e-government, jejaring sosial, media elektronik, website, dan lain sebagainya.[34] Apabila melihat dari sisi struktur hukum, regulasi di Indonesia telah mengatur perlindungan data pribadi melalui UU PDP, UU ITE, hingga peraturan pendukung terkait Pusat Data Nasional. Namun masih terdapat kelemahan adanya tumpang tindih kewenangan antar lembaga. Tingkat kesadaran dan kepatuhan penyelenggara sistem elektronik khususnya di Pusat Data Nasional maupun masyarakat terhadap pentingnya menjaga kerahasiaan data masih rendah, sehingga seringkali keamanan data dipandang sekadar formalitas, bukan kebutuhan strategis. Sementara itu juga masih ditemukan kurangnya koordinasi antar lembaga, serta konsistensi penerapan sanksi bagi pelaku peretasan maupun pihak yang lalai menjaga data. Ketiga struktur ini menunjukkan bahwa kebocoran data di Pusat Data Nasional bukan hanya persoalan teknis, tetapi juga persoalan fasilitas dan sumber daya manusianya.[35]

[34] Esther Hanaya, "Perlindungan Data Pribadi Di Era Digital Dalam Perspektif Perbandingan Hukum, *Jurnal Bevinding*, Vol. 1, No. 9, 2023, hlm. 13

[35] Diskominfo Kota Lhokseumawe, "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomeware", https://kominfo.lhokseumawekota.go.id/berita/read/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware-202407051720150165 , Juli 2024, dikutip 04 Agustus 2025

3. Alur Pemikiran



Ancaman yang timbul pada data dan informasi pusat data nasional yang menjadi tanggung jawab pemerintah antara lain Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara, Kepolisian Republik Indonesia, Tentara Nasional Indonesia serta stakeholder yang turut berkolaborasi menjaga ruang siber hingga seluruh masyarakat yang perlu menyadari bahwa perlindungan data dan informasi pribadi merupakan hal yang sangat penting. Di Indonesia sendiri ada beberapa regulasi kebijakan yang membawahi perlindungan data pribadi, tertuang pada UU PDP, Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Indonesia, dan UU ITE.

Berlandaskan permasalahan di atas tentang ancaman serta serangan data dan informasi yang terjadi di Pusat Data Nasional timbul pertanyaan bahwa apakah sudah cukup efektif dalam perlindungan data informasi di Pusat Data Nasional melihat ada beberapa regulasi yang memang dirancang untuk melindungi data pribadi serta bagaimana strategi yang akan dilakukan Indonesia di masa mendatang terhadap perlindungan data nasional. Dari keresahan serta pertanyaan tersebut apakah evaluasi dari sistem, sumber daya serta kebijakan yang ada dalam menangani perlindungan data, kemudian yang pada akhirnya meningkatkan kapasitas keamanan siber khusus nya di Pusat Data Nasional maupun Indonesia agar tidak kembali terjadi kebocoran data, yang dimana data merupakan hal vital.

Undang-undang yang menjadi payung hukum utama dalam menjaga keamanan, integritas serta kerahasiaan data memiliki banyak urgensi yang dapat memberi kepastian hukum, melindungi hak privasi warga negara, dan menetapkan tanggung jawab kepada pengendali data. Sebagai pengelola kebijakan Kementerian Komunikasi Dan Digital berperan dalam penyusunan regulasi teknis dan pengawasan keamanan siber. Kewenangan yang bertanggung jawab atas pengamanan infrastruktur informasi dalam mendeteksi, menganalisis, dan merespon insiden siber termasuk peretasan menjadi ranah Badan Siber Sandi Negara, melalui Direktorat Tindak Pidana Siber Kepolisian Republik Indonesia dan Tentara Nasional Indonesia dilakukan penyelidikan dan penindakan atas pelaku peretasan dan kejahatan siber. Kolaborasi antara stakeholder dan pemerintah sangat krusial dalam menjaga pertahanan negara khususnya perlindungan data di Pusat Data Nasional, mulai dari pengelolaan, pengawasan, hingga penanggulangan

insiden keamanan data. Tidak menutup untuk berkolaborasi dengan sektor swasta untuk mempercepat transfer teknologi dan keahlian teknis. Penguatan regulasi dan kebijakan terkait aturan perlindungan data pribadi termasuk pengawasan ketat terhadap lembaga yang mengelola dan memproses data. Kolaborasi dijalankan secara adaptif terhadap perkembangan teknologi dan ancaman siber.

E. Metode Penelitian

Metode penelitian merupakan kumpulan prosedur, skema, dan algoritma yang digunakan sebagai alat ukur atau instrumen dalam pelaksanaan penelitian.[36] Pendekatan dalam penelitian ini yaitu pendekatan kualitatif dengan metode penelitian yang digunakan adalah metode penelitian yuridis normatif, yaitu penelitian yang digunakan untuk mengkaji atau menganalisis data sekunder berupa bahan-bahan hukum, terutama bahan-bahan hukum primer dan sekunder.[37] Masalah yang akan dikaji mengacu terhadap ketentuan Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Indonesia, UU PDP, UU ITE serta aturan-aturan lain yang berkaitan dengan permasalahan yang akan dibahas pada penelitian ini. Kemudian penelitian ini menggunakan *survey* berdasarkan data terbaru terkait peretasan data di Pusat Data Nasional dan di Indonesia.

1. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini data primer dan sekunder, yaitu data normatif, yang terdiri dari:

a. Data Primer

Data primer adalah data yang diperoleh secara langsung dari sumber data yang mengacu pada peraturan perundang-undangan antara lain UU ITE, UU PDP dan Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data

[36] Kris H. Timotus, 2017, *Pengantar Metodologi Penelitian,* (Yogyakarta : Andi), Hlm.5
[37] Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum Dan Jurimetri*, (Jakarta : Ghalia Indonesia, 1998), Hlm. 11-12

Indonesia. Data ini diperoleh dengan mengumpulkan data-data yang berkaitan dengan kebocoran data di Pusat Data Nasional, kemudian dianalisis berdasarkan regulasi serta kebijakan yang ada.

b. Data Sekunder

Data sekunder ini dilakukan dengan penelitian kepustakaan guna mendapatkan landasan teoritis yang dibutuhkan untuk mendukung penelitian ini. Pengumpulan data dilakukan melalui studi atau penelitian kepustakaan *(library research)*, yaitu dengan mempelajari peraturan-peraturan, dokumen-dokumen serta buku-buku yang berkaitan dengan permasalahan yang akan diteliti namun tidak terbatas pada pendapat para akademisi dan para sarjana.

1) Bahan hukum primer, yakni UU ITE, UU PDP dan Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.
2) Bahan hukum sekunder, yakni jurnal/literatur/buku-buku yang berkaitan dengan analisis yuridis perlindungan hukum terhadap peretasan data pada pusat data nasional.
3) Bahan hukum tersier, yakni kamus hukum atau ensiklopedi hukum yang disertai analisis hukum berkaitan dengan perlindungan hukum terhadap data dan informasi pribadi.

2. Metode Pengumpulan Data

Data dalam penelitian ini dikumpulkan menggunakan cara studi pustaka, yang kemudian hasil penelitian ini dikumpulkan secara kualitatif.[38] Dengan berfokus pada studi kepustakaan atau rugulasi hukm tertulis, seperti Perpres Satu Data Indonesia, UU PDP, UU ITE.

[38] Burhan Ashshofa, *Metode Penelitian Hukum,* (Jakarta: Rineka Cipta, 2010), Hlm. 58

3. Metode Pengolahan Data

a. Identifikasi data, yaitu dengan mencari dan menetapkan data yang berkaitan dengan analisis yuridis perlindungan hukum terhadap peretasan data pada Pusat Data Nasional.
b. Pemeriksaan data, yaitu melakukan koreksi terhadap data yang diperoleh, apakah data tersebut benar dan lengkap serta sesuai dengan permasalahan yang dibahas.
c. Seleksi data, yaitu memeriksa keseluruhan data untuk menghindari kekurangan dan kesalahan data yang berhubungan dengan permasalahan.
d. Penyusunan data, dilakukan dengan cara menyusun data yang telah dikumpulkan secara sistematis dan efisien dengan bidang pembahasan.

4. Analisis Data

Analisis data dilakukan secara kualitatif sesuai dengan kebutuhan yang telah ditentukan dengan cara menafsirkan data berupa narasi yang diperoleh dari hasil pengumpulan data. Setelah dilakukan penafsiran data kemudian hasil data diuraikan secara sistematis untuk penyusunan kesimpulan. Analisis terdiri dari tiga alur kegiatan yang terjadi bersamaan yaitu: reduksi data, penyajian data, dan penarikan kesimpulan atau verifikasi.[39]

[39] Matthew B. Miles, A. Michael Huberman, *Analisis Data Kualitatif*, Jakarta: Universitas Indonesia, 2001), Hlm. 15

II. TINAJUAN PUSTAKA

A. Regulasi Dan Kebijakan Perlindungan Data

Secara harfiah data merupakan bentuk jamak dari kata *"datum"* yang dalam bahasa latin bermakna sebagai bagian informasi atau dengan kata lain data dapat dipahami sebagai kumpulan dari *datum-datum* yang melahirkan suatu informasi. Data harus pula memuat sekelompok fakta dalam bentuk simbol-simbol seperti alfabet, angka, citra maupun symbol khusus lainnya yang merepresentasikan ide, objek, kondisi atau situasi yang dapat disusun untuk diolah dalam bentuk struktur data, struktur *file*, dan *database*. Seiring dengan berkembangnya cara pengumpulan suatu data, maka beragam variable jenis data, *inter alia*, data primer-sekunder, data kualitatif-kuantitatif, hingga data pribadi, lahir dengan sendirinya.[40] Era digital yang semakin maju, pengumpulan, penyimpanan, dan penggunaan data telah menjadi hal yang umum. Regulasi perlindungan data bertujuan untuk mmberikan perlindungan yang memadai terhadap informasi individu, termasuk catatan kejahatan, dari penyalahgunaan atau akses yang tidak sah.

Dalam UU ITE disebutkan secara implisit mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. pengaturan tersebut terkait mengenai perlindungan dari tindakan penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses intervensi ilegal. Salah satunya dalam Pasal 26 UU ITE yang mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapatkan persetujuan pemilik data yang bersangkutan. Sehingga, pelanggaran atas tindakan tersebut dapat digugat atas kerugian yang ditimbulkan. Dalam penjelasan Pasalnya dikatakan bahwa Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi *(privacy rights)*. Selain itu dalam ketentuan Pasal 43 ayat (2) juga disebutkan esensi perlindungan data pribadi warga negara, meski dalam proses

[40] Wahyudi Djafar, "Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia", *Lembaga Studi Dan Advokasi Masyarakat*, 2016, Hlm. 3

pidana sekalipun. Dikatakan dalam ketentuan tersebut, bahwa dalam setiap penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik haruslah dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran pelayanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan. [41]

Muncul pertimbangan antara kebutuhan akan privasi individu dan kepentingan masyarakat dalam pencegahan kejahatan dan penegakan hukum.[42] Dalam upaya perlindungan terhadap data, dikenal istilah *data protection*. *Data protection* secara umum didefinisikan sebagai hukum yang dibuat untuk melindungi data. Maka, sangat penting bagi dibentuknya hukum perlindungan data untuk mengatur kegiatan seluruh stakeholder yang berperan aktif. Namun, tidak adanya peraturan dapat memberikan kemudahan terhadap kegiatan eksploitasi data yang dapat dilakukan oleh pihak lain. Keberadaan kerangka perlindungan data dapat memajukan individu, menghalangi praktik perusahaan data dan membatasi eksploitasi data. Kerangka perlindungan juga dapat memberikan kerangka pengelolaan secara nasional dan global untuk memastikan individu memiliki jaminan terhadap hak data yang mereka miliki. Konsep perlindungan data sering dianggap sebagai bagian dari perlindungan privasi. Indonesia, Malaysia, dan Vietnam menjadi hotspot serangan siber. Indonesia yang menjadi target dan tempat bagi dilaksanakannya serangan siber.[43]

Berdasarkan banyaknya kasus-kasus kebocoran data pribadi yang terjadi, menunjukkan bahwa hak atas privasi warga negara Indonesia sangat rentan untuk disalahgunakan, sehingga dapat merugikan masyarakat. Selain itu, pelanggaran data pribadi tidak hanya diakibatkan oleh kebocoran data pribadi. Hukum Uni Eropa (EU) memiliki pandangan terhadap data pribadi sebagai setiap informasi yang berkaitan dengan orang hidup yang dapat diidentifikasikan. Data pribadi dilindungi dengan cara apa pun. Hukum Uni Eropa juga tidak mementingkan cara penyimpanan data tersebut, baik secara tertulis maupun secara digital. Pada intinya,

[41] Wahyu Djafar, 2016, *Perlindungan Data Pribadi*, (Jakarta: Elsam), Hlm. 40

[42] Fauzi Anshari Sibarani, Sekar Ayu Diningrum, "Regulasi Perlindungan Data Pribadi Terhadap Catatan Kejahatan Dalam Perspektif Hak Asasi Manusia", *Jurnal Sanksi,* Vol 3, No 1 2021, Hlm.261

[43] Wisnu Handi Prabowo, "Perlindungan Data Personal Siber Di Indonesia", *Jurnal Internasional Padjajaran*, Vol 1, No.3, Januari 2020, Hlm. 228

semua data pribadi dilindungi melalui *General Data Protection Regulation* (GDPR). Semua anggota *European Un*i wajib membentuk instansi yang menjalankan urusan mengenai perlindungan data pribadi *Data Protection Agency* "DPA". *Data Protection Agency* merupakan lembaga pemerintahan independen yang melakukan supervisi terhadap implementasi peraturan yang mengatur mengenai perlindungan data pribadi. *Data Protection Agency* dibentuk untuk menindaklanjuti keluhan terhadap pelanggaran-pelanggaran dalam *General Data Protection Regulation*. Data pribadi didefinisikan sebagai informasi yang berkaitan dengan seseorang, baik berhubungan dengan kehidupan pribadi, profesional, dan publiknya.[44]

UN Cyber Convention atau Konvensi PBB tentang Kejahatan Siber masih dalam tahap pembahasan dan dikirim ke negara anggota untuk diputuskan apakah akan disepakati atau tidak disepakati sesuai dengan kebijakan masing-masing negara anggota. Konvensi ini mngatur pencegahan, kerjasama internasional, serta penegakan hukum terkait kejahatan siber lintas negara. Indonesia telah menyaksikan peningkatan eksponensial dalam penggunaan internet dan transaksi digital, yang disertai dengan peningkatan ancaman siber. Meskipun telah diberlakukannya peraturan domestik seperti UU ITE, masih terdapat kesenjangan dalam menangani kompleksitas kejahatan siber transnasional dan memastikan keselarasan yang memadai dengan standar internasional.[45] Adapun WIPO atau *World Intellectual Property Regulation* yang mengatur aspek hak kekayaan intelekutual termasuk ranah digital. WIPO dilakukan dengan kerjasama antar pemerintahan yang diadakan setiap tahun. Arah kebijakan yang awalnya lebih banyak bicara pada saat ini lebih menuju transparansi, karena informasi terkait sumberdaya hayati dan pengetahuan tradisional yang digunakan dalam paten dan harus dibuka saat pendaftarannya merupakan proses yang sangat meguntungkan bagi masyarakat pengahsil sumber daya genetik dan pengetahuan nasional.[46]

---

[44] Guswan Hakim, Jabalnur, Dkk, "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia", *Haluleo Legal Research*, Vol 5, No.2, Agustus 2023, hlm. 446

[45] Andi Rania Risya, "Kajian Teoritis Implikasi *The United Nations Convention Against Cybercrime* Terhadap Pengaturan Tindakan Pidana Siber Indonesia", *Jurnal Ikraith Humaniora*, Vol.9, Nomor 2, Juli 2025, hlm. 344

[46] Dayu Medina, "Perlindungan Sumber Daya Genetik Dan Pengetahuan Tradisional Dalam Kerangka WIPO", *Jurnal Das Sollen*, Vol. 01, Nomor 1, Juni 2024, hlm 177

Di Amerika Serikat bahkan belum ada undnag-undang privasi federal seketata GDPR, namun negara ini memakai regulasi sektoral seperti *Health Insurance Portability and Accountability* (HIPAA) yang melindungi informasi kesehatan yang dapat diidentifikasi secara pribadi. Regulasi ini menetapkan standar untuk perlindungan data pasien, termasuk penggunaan dan pengungkapan data dalam konteks penelitian dan pengembangan teknologi kesehatan.[47] Sedangkan di Cina memiliki *Personal Information Protection Law* dan regulasi yang ketat tentang keamanan data serta kontrol arus data lintas batas.

1. Perlindungan Hukum Terhadap Data Pribadi

Untuk mencapai keseimbangan atau keadilan dalam hukum, perlindungan hukum berarti hukum diharuskan menyambung serta menyelaraskan semua kepentingan masyarakat, juga memberi batasan atas kepentingan beberapa pihak lain. Persetujuan ataupun kesepakatan keseluruhan elemen masyarakat guna mengatur keseluruhan kaitan serta perilaku antar anggota masyarakat sertaantar masyarakat dengan pemerintah menyebabkan terjadinya perlindungan hukum. Philip M. Hadjon menyampaikan bahwasanya perlindungan hukum berarti menjaga harkat dan martabat juga mengakui hak asasi manusia yang dipunya oleh subjek hukum. Perlindungan ini diberi berdasar atas ketentuan hukum yang diberlakukan, baik sebagai bentuk kekuasaan yang sah maupun sebagai kumpulan aturan atau pun norma yang fungsinya guna melindungi sesuatu dari gangguan atau ancaman lainnya.[48]

Jika dilihat dari sarananya perlindungan hukum dibagi menjadi dua, yaitu sarana perlindungan hukum preventif dan sarana perlindungan hukum represif. Menurut Philipus M Hadjon dengan bukunya yang berjudul Pelindungan Hukum Bagi Rakyat Indonesia, Penanganannya dan Pengadilan Dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara, di Indonesia

[47] Susy Ariyanie Yusuf, "Aspek Legal dan Etika Penggunaan Data Pasien Dalam Teknologi *Big Data* dan Kecerdasan Buatan di Sektor Kesehatan", *Jurnal Masyarakat Hukum Kesehatan Indonesia*, Desember 2024, hlm. 385

[48] Nabiha Khansa Rusyada, "Perlindungan Hukum Terhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022", *Jurnal Hukum DesentralisasiI,* Vol.2, No.3, Agustus 2025, hlm. 258

belum ada pengaturan secara khusus mengenai sarana perlindungan hukum preventif. Philipus M Hadjon dalam bukunya juga lebih menitikberatkan kepada sarana perlindungan hukum yang represif, seperti penanganan perlindungan hukum di lingkungan Peradilan Umum. Ini berarti bahwa perlindungan hukum baru diberikan ketika masalah atau sengketa sudah terjadi, sehingga perlindungan hukum yang diberikan oleh Peradilan Umum bertujuan untuk menyelesaikan sengketa. Begitu juga dengan teori-teori lain yang menyinggung tentang perlindungan hukum juga membahas sarana perlindungan hukum yang bersifat represif.[49]

Berdasarkan dasar hukum tersebut, maka hak privasi terhadap data pribadi harus ditegakkan karena pada dasarnya perlindungan terhadap data pribadi merupakan Hak Konstitusional warga negara Indonesia. Hak konstitusional adalah kewajiban bagi negara untuk memberikan perlindungan secara hukum untuk aspek kehidupan masyarakat Indonesia. Hak konstitusional harus didapatkan oleh setiap warga negara Indonesia. Hak konstitusional harus memiliki tujuan hukum yaitu kepastian hukum, keadilan hukum dan kemanfaatan hukum. Dengan dasar hukum tersebut juga beberapa peraturan perundang – undangan di Indonesia mengatur secara tersirat mengenai perlindungan data pribadi.

Perlindungan Hukum terhadap Data Pribadi tercipta karena maraknya akan pelanggaran terhadap data pribadi seseorang maupun badan hukum. Penyalahgunaan data pribadi dapat menimbulkan kerugian yang tidak hanya pada materiil saja, tetapi moral juga dirugikan terkait hal ini yakni nama baik dan kehormatan seseorang atau lembaga terlecehkan. Sejak dikemukakan untuk pertama kalinya oleh Samuel Warren and Louis Brandeis dari Amerika Serikat, yang berpendapat bahwa ada satu hak dasar manusia yang harus dilindungi yang disebut dengan *The Right to Privacy*. Jadi privasi adalah hak untuk menikmati hidup dan menuntut hukum untuk melindungi privasi, selanjutnya menurut Warren, karena ada perkembangan teknologi, ekonomi dan politik maka ada hak baru yang belum dilindungi oleh *Common Law.* Alasan privasi harus dilindungi

[49] Bisri Fadil Hasan, "Perlindungan Hukum Data Pribadi Terhadap Konsumen Pinjaman Berbasis Online", *Skripsi,*Univeritas Syarif Hidayatullah Jakarta, 2023, hlm. 31

yaitu: Pertama, dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. Kedua, seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*) sehingga privasi sangat diperlukan oleh seseorang. Ketiga, privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hal ini akan hilang, apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik, termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutkan sebagai *the right against the world*. Kelima, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya, sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapatkan kompensasi.[50]

Apabila kita melihat akhir-akhir ini, banyak kasus yang menimpa masyarakat terhadap peretasan data pribadi mereka oleh pihak yang tidak bertanggung jawab. Pengaturan berkenaan mengenai Perlindungan Data Pribadi di Indonesia masih bersifat umum dan tidak mengakomodir berbagai isu permasalahan yang sering terjadi pada masyarakat serta terletak secara terpisah dalam berbagai peraturan perundang-undangan. Dengan tersedianya pengaturan yang secara khusus dan komprehensif, dirasakan Indonesia dapat lebih siap menghadapi tantangan mengenai persoalan data pribadi. Dalam hal ini, sudah menjadi suatu kewajiban dan sejatinya negara hukum sebagaimana tercantum dalam Pasal 1 ayat (3) Undang-Undang Dasar 1945 bahwa negara Indonesia adalah negara hukum. Artinya bahwa Indonesia adalah sebuah negara yang berlandaskan hukum dan juga demokratis yang harus memberikan perlindungan hukum terhadap warga negaranya dalam konteks persoalan perlindungan data pribadi. Dalam hal ini, regulasi atau peraturan perundang-undangan terkait

[50] Dhoni Martien, 2023, *Perlindungan Hukum Data Pribadi*, (Makassar: Mitra Ilmu), hlm.35

Perlindungan Data Pribadi di Tanah Air dirasa belum cukup menjawab tantangan terhadap Perlindungan Data Pribadi yang begitu besar. Kemudian masyarakat mendesak agar dibentuknya peraturan dalam bentuk Undang-undang mengenai Perlindungan terhadap Data Pribadi.[51]

Disahkannya UU PDP menjadi suatu harapan perlindungan hukum dari banyaknya kasus kejahatan dari penyalahgunaan data pribadi di Indonesia yang berasal dari kebocoran-kebocoran data serta pencurian data pribadi. Hadirnya UU PDP memberi kewenangan kepada pemerintah dalam mengawasi tata kelola data pribadi yang dilakukan oleh penyelenggara sistem elektronik. Dalam UU PDP dinyatakan mengenai data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Sedangkan yang dimaksud dengan perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Agar perlindungan data pribadi dapat dilakukan dengan tepat memenuhi semua kriteria dalam pengaturannya, UU PDP membagi data pribadi kedalam dua jenis data, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Sebagaimana yang tercantum didalam Pasal 4 ayat (2), jenis data pribadi yang bersifat spesifik tersebut meliputi: data informasi; data biometrik; data genetika; catatan kejahatan; data anak; data keuangan pribadi; data lainnya sesuai dengan ketentuan perundang-undangan.

Upaya pengaturan terkait hak privasi atas data pribadi merupakan perwujudan atas pengakuan dan perlindungan hak-hak dasar manusia. Keberadaan UU PDP telah mewujudkan cita hukum dalam melindungi masyarakat baik secara normatif dan konstitutif. Dengan memberikan perlindungan terhadap hak pribadi tersebut, berarti juga memberikan perlindungan terhadap hak atas kebebasan berbicara yang menjamin perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu

[51] Endison Ravlindo, Ariawan Gunadi, "Perlindungan Hukum Terhadap Data Kesehatan Melalui Pengesahan Rancangan UU PDP", *Jurnal Hukum Adiguna*, Vol 4, Nomor 2, Desember 2021, hlm. 4757

yang merupakan hak asasi. Konsep perlindungan data pribadi ini menekankan bahwa setiap orang berhak untuk memutuskan ketika seseorang akan memberikan data kepada orang lain atau untuk berbagi data kepada orang lain serta menentukan kondisi yang harus dipenuhi selama proses berbagi data dalam sebuah komunitas.[52]

Data pribadi yang kita/pengguna himpun ke dalam sistem elektronik bersifat rahasia dan wajib dilindungi. Penyelenggara Sistem Transaksi Elektronik/*platform* wajib menjaga keutuhan, kerahasiaan data tersebut dari *hacker*/ peretas dan menjamin untuk tidak disalahgunakan, dijual. Penulis juga menghimbau seyogyanya aplikator melakukan *double check* terhadap data pribadi misalnya dengan menelpon pemilik data pribadi tersebut karena dewasa ini modus penipuan online, oknum dapat dengan mudah mendapatkan data pribadi kita di internet, menggunakanya seolah-olah itu adalah data pribadinya. Pengaturan data pribadi yang ideal adalah peraturan yang mengikuti perkembangan zaman berlandaskan nilai-nilai filosofis, landasan sosiologis dan landasan yuridis. Walaupun media data pribadi adalah teknologi komputer, internet dan sistem elektronik namun wajib tetap berlandaskan nilai-nilai kejujuran, nilai tanggung jawab, dan nilai saling menghargai. Pengaturan data pribadi yang ideal berangkat dari fakta empiris bahwa data pribadi masih banyak disalahgunakan, oknum yang bekerja atau menguasai informasi teknologi melakukan *'knock down'* yang bermuatan melawan hukum.

Perumusan aturan tentang Privasi atas Data Pribadi dapat dipahami karena adanya kebutuhan untuk melindungi hak-hak individu di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, penyelenggaraan, penyebarluasan data pribadi. Perlindungan yang memadai atas privasi menyangkut data dan pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data dan informasi pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya. Dengan demikian, pengaturan ini akan menciptakan keseimbangan antara hak-hak individu dan masyarakat yang diwakili kepentingannya oleh

[52] Riyantika Pratiwi, Tri Novita Sari Manihuruk, Irwan Harapah, "Tinjauan Yuridis Perlindungan Data Pribadi Dalam Transaksi E-Commerce", Jurnal Pagaruyung, Vol 7, No 2, Januari 2024, hlm. 375

negara. Pengaturan tentang privasi atas data dan informasi pribadi ini akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi.[53]

2. Teori Strategi Keamanan *Cyber* Atau Data Informasi

Saat ini data informasi merupakan sumber aset yang begitu penting dan sangat berharga bagi keberlangsungan hidup suatu lembaga organisasi, perusahaan/bisnis, pertahanan keamanan dan keutuhan serta kedaulatan sebuah negara, di mana kepercayaan masyarakat dan konsumen menjadi indikator integritas suatu organisasi tersebut. Untuk menjaga kepercayaan publik maka sebagai organisasi harus mampu menjaga ketersediaan data informasi, ketepatan dan kebutuhan informasinya. Di era digital saat ini, semakin mudahnya mengakses informasi melalui layanan internet menyebabkan informasi sangat mudah diperoleh dan disebarluaskan, sehingga informasi memiliki nilai dan harus dilindungi, karena keamanan data informasi sudah menjadi prioritas.[54] Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep *cyber security* atau keamanan siber. Karena *cyberspace* merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Maka konsep keamanan siber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.[55] Menurut Ghernaouti-Helie, seiring dengan semakin meningkatnya penggunaan sistem infrastruktur penting oleh suatu negara, ancaman terhadap keamanan *cyber security* juga meningkat.

Ancaman ini bisa berasal dari kegiatan kriminal atau non-kriminal, disengaja atau tidak disengaja. Oleh karena itu, infrastruktur telekomunikasi, layanan, dan aktivitas harus dikelola dengan standar keamanan yang tinggi untuk melindungi keamanan, ekonomi, keamanan publik, dan kesehatan dari risiko. Mekanisme mengenai keamanan harus dapat melindungi informasi secara

---

[53] Rizky P.P. Karo Karo, 2020, *Pengaturan Perlindungan Data Pribadi Di Indonesia,* (Bandung: Nusa Media), hlm. 58

[54] Ika Yusnita Sari, Dkk, 2020, *Keamanan Data Dan Informasi,* Kisaran: Yayasan Kita Menulis, hlm. 104

[55] Dewi Triwahyuni, Tine Agustin, "Strategi Keamanan Cyber Amerika Serikat", *Jurnal Ilmu Politik Dan Komunikasi,* Vol 6, No 1, Juni 2016, hlm. 110

efektif dan efisien, tentu hal ini dapat dimulai dari pengamanan terhadap *physical attack* maupun *cyberattack*, dimana *cybersecurity* disini merupakan upaya untuk melindungi aset baik informasi maupun infrastruktur dari ancaman *cyber attack*, elemen-elemen pokok *cybersecurity* yang perlu diperhatikan adalah:

a. *Security Policy*

   Dimana harus memuat standar yang dapat digunakan sebagai pedoman dalam melakukan proses yang berhubungan dengan keamanan informasi.

b. *Information Infrastructure*

   Adalah informasi yang mencakup media dalam menjalankan operasi informasi, termasuk hardware dan jaringan. Contoh Contohnya meliputi router, switch, server, sistem operasi, database, dan website.

c. *Perimeter Defense*

   Merupakan media yang berfungsi sebagai elemen pertahanan dalam melindungi infrastruktur informasi yang dimiliki. Contohnya adalah *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan *firewall*.[56]

d. *Network Monitoring System*

   Merupakan alat yang berfungsi untuk memantau kualitas, pemakaian, dan kinerja dari infrastruktur informasi.

e. *System Information And Event Management*

   Merupakan media yang sangat berperan dalam memonitor kejadian yang mengancam jaringan termasuk kejadian yang terkait dengan insiden keamanan.

f. *Network Security Assessment*

   Merupakan elemen pendukung dalam *cybersecurity*, dimana ini berperan sebagai mekanisme kontrol terhadap kualitas pengamanan dari keamanan informasi.

[56] Universitas Pertahanan RI, Hlm. 18

g. Human Resource Dan Security Awareness

Harus ditanamkan kepada seluruh sumber daya manusia pada lembaga yang berkaitan dengan keamanan informasi.[57]

Dalam konteks keamanan siber, awal mula hukum Indonesia yang mulai bergerak pada bidang keamanan teknologi dan informasi bisa dilacak dengan diberlakukannya Undang-Undang Telekomunikasi Nomor 36 Tahun 1999 dan UU ITE. Kedua undang-undang ini dihitung sebagai bentuk kebijakan dari pemerintah Indonesia mengenai keamanan jalur komunikasi teknologi pada umumnya di Indonesia. Ditandatangani oleh Presiden RI Bacharuddin Jusuf Habibie dan Menteri Sekretaris Negara Muladi, Undang-Undang Telekomunikasi merupakan salah satu contoh pertama dari dibentuknya sebuah kebijakan khusus tentang kegiatan telekomunikasi di Indonesia (DPR RI, 1999). Undang-undang ini membahas semua bentuk komunikasi yang menggunakan teknologi komunikasi pada masanya seperti televisi, radio, telepon, dan lain sebagainya.

UU ITE mengakui peran internet sebagai sarana komunikasi dan secara eksplisit membahas informasi elektronik, transaksi elektronik, dan dokumen elektronik. Namun, kritik muncul terkait ketidakcukupan kedua undang-undang tersebut dalam menegakkan keamanan siber. Undang-Undang Telekomunikasi tidak mencakup jaringan internet sebagai media komunikasi, sulitnya mengatasi kasus hukum berbasis internet. UU ITE, meskipun signifikan, masih memerlukan dukungan beberapa undang-undang lain seperti Undang-Undang Perlindungan Konsumen, Undang-Undang Hak Cipta, dan Undang-Undang Pornografi untuk efektif beroperasi. Kelemahan cakupan definisi dan hukuman terhadap *cybercrim*e di Indonesia menjadi sorotan. Pembentukan lembaga keamanan yang relevan untuk keamanan siber yaitu *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII). Ini mencerminkan kesadaran akan pentingnya lembaga khusus untuk menangani isu keamanan siber di Indonesia. Tugas dan fungsi *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) mencakup pemantauan, pendeteksian dini, peringatan terhadap ancaman jaringan, serta kerja sama dengan pihak

[57] *Ibid*, Hlm. 19

dalam dan luar negeri. Secara umum, kerangka hukum keamanan siber di Indonesia dibangun berdasarkan UU ITE, Peraturan Pemerintah Nomor 82 Tahun 2012, dan regulasi menteri. Namun, terdapat permasalahan nasional terkait keamanan siber, seperti lemahnya pemahaman pemangku kepentingan terhadap security di dunia siber, kebutuhan legalitas yang memadai dalam menangani serangan siber, tata kelola kelembagaan yang parsial, serta kelemahan industri dalam mengembangkan perangkat keras terkait teknologi informasi.

Dalam upaya pemerintah Indonesia untuk membangun awareness tentang penegakan keamanan siber, pendidikan tentang keamanan siber secara spesifik juga belum dilaksanakan di Indonesia dengan mencukupi. Walaupun begitu, perkembangan sebuah lembaga khusus di bidang keamanan siber di Indonesia pun terus dilanjutkan yang berujung dengan dibentuknya Badan Siber dan Sandi Negara pada tahun 2017. Perlindungan hak individu di ranah siber diakui sebagai krusial, namun kekurangan regulasi, terutama Undang-Undang tentang keamanan siber, membuat penegakan keamanan ini menjadi sulit dilakukan. Dengan pelaku *cybercrime* yang tidak terikat oleh batasan geografis, penanganan *cyber threat* membutuhkan perhatian khusus. Meski prinsip ini diakui oleh pihak-pihak terkait di Indonesia, kekurangan undang-undang khusus tentang keamanan siber menjadi kendala utama dalam upaya penegakan keamanan di era digital ini.[58]

Legalitas penanganan kejahatan di dunia siber masih lemah karena meski telah ada peraturan perundang-undangan yang melarang bentuk penyerangan atau perusakan sistem elektronik, selanjutnya dalam UU ITE belum terdapat peraturan perundang-undangan yang mengatur secara khusus *cybercrime* dan penanganan *cybercrime* padahal di lain sisi bentuk kejahatan dunia cyber semakin meningkat dan pola kejadiannya sangat cepat sehingga sulit untuk ditangani oleh aparat penegak hukum. Pengembangan dan penguatan kebijakan *cyber security* di Indonesia hendaknya menyatu dengan strategi nasional dalam membangun ekosistem *cyber security* nasional yang telah disusun pemerintah.

[58] Yustika Citra, Dkk, "Strategi Penanganan Keamanan Siber Di Indonesia", *Jurnal Review Pendidikan Dan Pengajaran*, Vol 6, No 2, 2023, Hlm. 1944-1946

Strategi nasional dalam membangun ekosistem *cyber security* nasional yang telah disusun pemerintah tersebut meliputi upaya hukum, upaya teknis yang melingkupi standar dan operasional, penataan organisasi dan kelembagaan penanganan *cyber security* dalam lingkup kepentingan nasional, capacity building atau peningkatan kapasitas Sumber Daya Manusia di bidang *cyber security* dan meningkatkan kerjasama internasional. [59]

3. Teori Kedaulatan Dan Asas Kehati-Hatian Pada Data Nasional

Dalam perkembangannya, para akademisi mulai memberikan justifikasi teoritis kepada kedaulatan sebagai otoritas tertinggi dan absolut yang melekat pada negara. Tidak ada lagi otoritas yang lebih tinggi kepada suatu pemerintahan negara tertentu dan negara mengelola pemerintahan di dalam wilayah teritorialnya. Menurut Thomson (1995, 214), kedaulatan lebih tepat dipahami sebagai "Otoritas Negara", bukan "Kontrol Negara". [60] Dalam prakteknya, negara memerlukan perdagangan, aliran keuangan, dan investasi global. Globalisasi yang terus menguat sejak 1990-an membuat relasi antara negara dan batas-batas wilayah menjadi lebih kompleks. Ruang Siber *(cyberspace)* merupakan "Jaringan yang saling terhubung melalui infrastruktur teknologi informasi, termasuk internet, jaringan telekomunikasi, sistem komputer, serta prosesor dan pengontrol dalam industri penting".

Kemampuan suatu negara dalam menerima atau menolak suatu serangan sangat ditentukan oleh kapasitas pertahanan sibernya. Dalam konteks ruang siber, berbagai bentuk serangan informasi maupun peretasan data akan dengan mudah masuk dan mengganggu stabilitas apabila tidak tersedianya mekanisme penangkal atau sistem pertahanan yang memadai. Ruang siber menghasilkan kerapuhan dan saling ketergantungan dari negara yang memiliki komitmen terhadap ruang siber. Di saat yang bersamaan, perlu ditegaskan bahwa sekuat apapun internet menembus batas negara, hal itu tidak memberikan pengaruh

[59] Handrini Ardiyanti, "Cyber Security Dan Tantangan Pengembangannya Di Indonesia", *Jurnal Politica*, Vol, 5, No 1, Juni 2014, Hlm.102

[60] Arief Bakhtiar Darmawan, Dkk, "Kedaulatan Negara Dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook Dan Google", *Jurnal Hubungan Internasional*, Vol. 16, No. 1, Januari-Juni 2023, Hlm. 214

apapun terhadap integritas legal negara dalam hukum internasional. Oleh karena itu, posisi negara dalam hubungan internasional masih relatif kuat. [61] Terkait regulasi yang menjadi dasar atau pijakan pertahanan siber, diantaranya UU ITE. Selain itu, pemerintah juga telah merilis UU PDP. Regulasi perlindungan data pribadi di Indonesia tersebar pada berbagai macam sektor, seperti keuangan, kesehatan, kependudukan, telekomunikasi, perbankan, perdagangan dan lain-lain. UU PDP dinilai memberi landasan hukum bagi Indonesia untuk menjaga kedaulatan negara, keamanan negara dan perlindungan terhadap data pribadi milik warga negara Indonesia dimanapun data pribadi tersebut berada. Guna menghindari adanya serangan siber, perlu adanya penegakan negara dalam ruang digital. Direktur Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Digital, Semuel A. Pangerapan menyatakan tiga model pendekatan dan penegakan kedaulatan negara, yaitu: 1) *Data localization policies* (Data tidak bisa dipertukarkan dan hanya boleh ada di dalam negeri); 2) Efektivitas pengawasan dan penegakan hukum (Data bisa berada di luar negeri, tetapi disaat dibutuhkan pemegang data pribadi harus memberikan); 3) Kesetaraan hukum perlindungan data pribadi (Selama negara lain memiliki aturan terkait Perlindungan Data Pribadi yang setara dengan. Indonesia, maka data bisa dipertukarkan).[62]

Adapun dalam perspektif *cybersecurity*, menurut Nugraha Kautsarina & Sastrosubroto adalah pembentukan kedaulatan data (*data sovereignty*) Indonesia dengan fokus pada kerahasiaan data *(data confidentiality)*, keutuhan data *(data integrity)* dan keberadaan data *(data availability)* yakni melalui enkripsi, layanan email nasional, lokalisasi pusat data (data center), routing nasional pada trafik internet, infrastruktur *backbone* jaringan telekomunikasi nasional. Untuk itu, diperlukan penetapan wilayah siber Indonesia *(cyber territory)* yang dilakukan dengan menata konfigurasi jaringan *broadband* domestik (jaringan pita lebar) dan membangun gerbang pembatas antara jaringan *broadband* global dan nasional/domestik. Melalui pembatasan tersebut, negara dapat mengontrol

[61] *Ibid,* Hlm. 216

[62] Dede Suprayitno, Dkk, "Kebijakan Keamanan Siber Dan Kedaulatan Data: Suatu Kunci Dalam Mewujudkan Digitalisasi Pemilu Di Indonesia", *Jurnal Administrasi Publik,* Vol. 10, No. 1, April 2024, Hlm. 15-16

jaringan domestik dan global yang terkoneksi dengan gerbang nasional Indonesia. Dengan pembentukan *cyber territory*, negara menerapkan kedaulatan melalui pembentukan Gerbang Internet Nasional *(Internet National Gateway)*, sebagai pintu keluar masuk informasi dalam wilayah *cyber territory* Indonesia serta penempatan data center di dalam wilayah Indonesia.[63]

Asas kehati-hatian dalam konteks perlindungan data pribadi mengacu pada tindakan proaktif dan pencegahan yang diambil oleh pemerintah untuk memastikan bahwa data pribadi dikelola dan dilindungi dengan cara yang aman dan sesuai dengan peraturan perundang undangan yang ada. Hal ini mencakup berbagai tindakan preventif untuk mencegah pelanggaran data dan meminimalkan risiko penyalahgunaan data pribadi. Dalam UU PDP menetapkan adanya otoritas perlindungan data yang bertugas mengawasi kepatuhan terhadap undang-undang tersebut. Pemerintah dan lembaga terkait harus aktif melakukan edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi. Oleh karena itu, seluruh stakeholder, perlu mendapatkan pelatihan yang memadai tentang asas kehati-hatian dan praktik terbaik dalam pengelolaan data pribadi. Sehingga Indonesia perlu mengadopsi standar internasional dalam perlindungan data pribadi untuk memastikan bahwa perlindungan data di Indonesia sejajar dengan praktik terbaik global.

Karena dengan adanya kerjasama dengan negara lain dalam berbagi informasi dan teknologi terkait keamanan data dapat membantu meningkatkan perlindungan data pribadi di Indonesia sehingga kejadian peretasan yang yang baru-baru ini tidak terjadi. UU PDP telah mengatur bahwa perlindungan data pribadi seseorang dilaksanakan melalui beberapa asas, salah satunya yaitu asas kehati-hatian, asas kehati-hatian ini menjelaskan bahwa para pihak yang terkait dengan pemrosesan dan pengawasan data pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian. [64] Asas kehati-hatian pada pengelolaan data pribadi di Pusat Data Nasional wajib diterapkan secara menyeluruh oleh seluruh stakeholder, baik dari sisi pemerintah/regulator

[63] Siti Yuniarti, Erni Herawati, "Analisis Hukum Kedaulatan Digital Indonesia", *Jurnal Pandecta*, Vol.15, No.2, Desember 2020, Hlm. 161

[64] Andri Pranata, Dkk, "Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan UU PDPDi Era Digital 5.0", *Journal Of Law And Nation*, Vol.3, No.3, Agustus 2024, Hlm. 725

kebijakan, masyarakat, hingga lembaga perlindungan data seperti Kementerian Komunikasi dan Digital serta Badan Siber dan Sandi Negara. Pemerintah berkewajiban memastikan kebijakan yang jelas, penyediaan infrastruktur yang aman, serta audit berkala untuk mencegah risiko kebocoran. Regulator yang bertugas mengawasi kepatuhan terhadap standar keamanan, hingga kolaborasi dengan penegak hukum dalam menegakkan sanksi atas kelalaian, dan menjaga independensinya agar pengawasan berjalan objektif. Masyarakat sebagai pemilik data juga dituntut untuk lebih bijak dalam memberikan data pribadi, meningkatkan literasi digital, serta aktif menggunakan mekanisme pengaduan apabila terjadi pelanggaran atau kebocoran data. Sementara itu, lembaga Kementerian Komunikasi dan Digital serta Badan Siber dan Sandi Negara berperan sebagai pengawas yang menilai risiko, melakukan investigasi insiden, serta memberi edukasi dan advokasi terkait hak-hak perlindungan data pribadi.

Dengan strategi kolaborasi tersebut, asas kehati-hatian dapat menjadi penopang atau pondasi yang penting dalam menjaga keamanan dan kepercayaan publik terhadap pengelolaan data pribadi di Pusat Data Nasional. Seiring dengan kemajuan teknologi informasi, dunia menjadi lebih terbuka lebar. Secara khusus, pemerintah pun menerbitkan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.[65] secara institusi, Kementerian Pertahanan dan Tentara Nasional Indonesia memiliki dua kepentingan dalam pertahanan siber. Yakni untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya serta mendukung koordinasi pengamanan siber di sektor-sektor lainnya sesuai kebutuhan. Diantaranya kebijakan, kelembagaan, teknologi dan infrastruktur pendukung, serta sumber daya manusia. Hal terkait keamanan siber, turut berhubungan dengan upaya-upaya untuk menjaga kedaulatan data. Secara etimologi, kedaulatan merupakan kekuasaan tertinggi dan diambil dari bahasa Arab, yang berarti *daulah* dengan arti kekuasaan. Sementara dalam bahasa Latin disebut *supremus* dengan arti tertinggi. Dalam Kamus Besar Bahasa Indonesia kedaulatan juga berarti kekuasaan tertinggi atas pemerintahan, daerah dan sebagainya.

[65] Berita Negara Republik Indonesia Tahun 2014 Nomor 1712.

Berkaca dari amandemen ketiga Undang-Undang Dasar Negara Republik Indonesia 1945 yang dilaksanakan pada 2021, ketentuan Pasal 1 ayat 2 diamandemen menjadi: "Kedaulatan di tangan rakyat dan dilaksanakan menurut Undang-Undang Dasar." Hal yang sama juga berlaku pada definisi kedaulatan daa, yangs etara dengan kedaulatan bangsa. Pasalnya hal ini akan menyangkut perlindungan data pribadi, kepastian hukum, hak-hak dalam dunia digital termasuk diantaranya dalam bisnis yang bersinggungan dengan kelancaran akses ke masyarakat. Terkait regulasi yang menjadi dasar atau pijakan pertahanan siber diantaranya UU ITE. Sedangkan UU PDP dinilai memberi landasan hukum bagi Indonesia untuk menjaga kedaulatan negara, keamanan negara dan perlindungan terhadap data pribadi milik warga negara Indonesia dimanapun data pribadi tersebut berada. Guna menghindari adanya serangan siber, perlu adanya penegakan negara dalam ruang digital. Direktur Jenderal Aplikasi Informatika, Kementerian Komunikasi Dan Digital, Semuel A. Pangerapan menyatakan tiga model pendekatan dan penegakan kedaulatan negara, yaitu: 1) *Data Localization Policies* (data tidak bisa dipertukarkan dan hanya boleh ada di dalam negeri); 2) Efektivitas pengawasan dan penegakan hukum (data bisa berada di luar negeri, tetapi disaat dibutuhkan pemegang data pribadi harus memberikan); 3) Kesetaraan hukum perlindungan data pribadi (selama negara lain memiliki terkait perlindungan data pribadi yang setara dengan Indonesia, maka data bisa dipertukarkan). [66]

B. Kajian Umum Tentang Konsep *Indonesia Data Protection System* (IDPS) dan Pusat Data Nasional

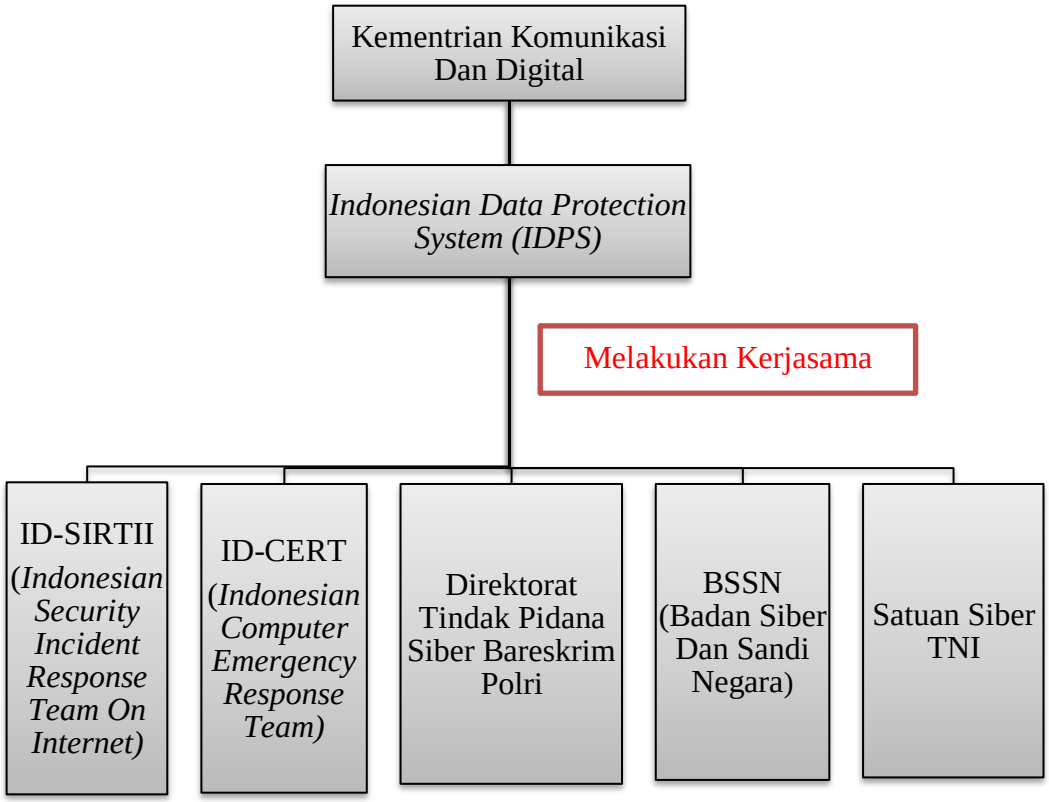
Saat ini Indonesia memiliki suatu konsep pengelolaan sistem yang mampu menjamin terlindunginya data pribadi yaitu, *Indonesian Data Protection System* (IDPS) yang merupakan suatu sistem yang mampu meminimalisir kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk mengamankan data pribadi seseorang pada central data atau pusat

[66] Dede Suprayitno, "Kebijakan Keamanan Siber Dan Kedaulatan Data: Suatu Kunci Dalam Mewujudkan Digitalisasi Pemilu Di Indonesia", *Jurnal Administrasi Publik*, Vol. 10, No. 1, April, 2024, Hlm. 14-15

pengumpulan data, selain itu *Indonesian Data Protection System* juga memastikan pengelolaan data dan informasi seseorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini. *Indonesian Data Protection System* sebagai sebuah sistem yang dilekatkan pada Kementerian Komunikasi dan Digital, untuk mendukung kinerja dari sistem ini juga perlu adanya kerjasama terhadap badan atau pun tim yang sudah dibentuk oleh pemerintah sebelumnya, kerjasama ini dilakukan untuk mewujudkan adanya *cyber surveillance* dan perlindungan data terhadap data dan informasi seseorang yang sedang diproses, fungsi dari adanya kerjasama ini adalah untuk lebih meningkatkan ketahanan dari *Indonesian Data Protection System* itu sendiri yang nantinya akan menjadi pusat pengelolaan data pribadi dan sebagai pusat kontrol data pribadi seseorang yang dilaporkan oleh pengelola data.[67]

Jika terjadi pelanggaran data pribadi, pengontrol data harus memberitahu subjek data yang terbatas sehingga Kementerian Komunikasi Dan Informasi dapat melakukan tindakan seperti pemberitahuan kepada publik jika ada dampak pada kasus tersebut. Meskipun UU PDP tidak menjatuhkan hukuman atas pelanggaran data pribadi, pengontrol data akan bertanggung jawab atas pemrosesan data pribadi mereka dan harus menunjukkan komitmen mereka terhadap penerapan prinsip-prinsip perlindungan data pribadi. Ini berarti pengontrol data harus memberikan kompensasi terhadap subjek data yang telah dirugikan oleh pelanggaran data pribadi. Berikut bagan mengenai mekanisme kerjasama *Indonesia Data Protection System* (IDPS):

[67] Muh Rifqy Hidayatullah Arham, M. Chaerul Risal, "Perlindungan Data Pribadi Bagi Pengguna Media Sosial", *Jurnal Al-Tasyriiyah,* Vol. 3, No. 2, 2023, Hlm. 115



Sistem *Indonesian Data Protection System* juga mampu mengatasi dan meminimalisir banyaknya kejahatan-kejahatan di bidang pengelolaan data dan informasi pribadi, yang diketahui bersama kejahatan terhadap pengelolaan data pribadi ini akan semakin meningkat seiring perkembangan teknologi yang begitu pesat, dan diperburuk dengan belum adanya regulasi yang mengatur mengenai perlindungan data pribadi dan kejahatan siber itu sendiri. Kepastian pengelolaan data dan informasi pribadi secara tepat dan baik diperlukan agar data pribadi seseorang tidak disalahgunakan, makan dari itu *Indonesian Data Protection System* sebagai sebuah sistem menjadi sebuah solusi dari permasalahan pengelolaan data dan informasi pribadi yang saat ini menjadi masalah di Indonesia. Hal ini ditunjukkan dengan identifikasi problematika yang telah diuraikan sebelumnya. Adapun beberapa keunggulan yang dimiliki oleh *Indonesian Data Protection System* yaitu adalah: (1) memastikan pengelolaan data dan informasi seseorang dilakukan secara tepat dan baik; (2) melakukan izin terlebih dahulu jika data dan informasi seseorang akan digunakan kepada pemiliknya dengan jangka waktu yang

ditentukan; (3) memiliki pengontrol data yang dimana sebagai pusat pengelolaan data yang langsung mengkoordinasikannya ke pusat dengan waktu sekali dalam 24 jam; (4) adanya kerjasama Kementerian Komunikasi dan Digital dengan lembaga keamanan siber untuk lebih memastikan dan meningkatkan pengawasan dan kontrol data; dan (5) meminimalisir adanya penyalahgunaan data dan informasi pribadi seseorang oleh pihak ketiga, karena adanya pengontrol data yang ditempatkan di perusahaan dan institusi pemerintah.[68]

Pusat Data Nasional merupakan infrastruktur teknologi yang berfungsi untuk mengelola, menyimpan, serta melindungi data dari berbagai instansi pemerintah secara terpusat. Seiring dengan meningkatnya kebutuhan digitalisasi dan pengintegrasian layanan publik melalui konsep e-government, keberadaan PDN menjadi fondasi utama dalam mendorong pemerintahan yang lebih efisien, aman, dan transparan di era transformasi digital. Pusat Data Nasional (PDN) memiliki peran strategis dalam mendukung implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia. Sebagai infrastruktur utama, PDN berfungsi sebagai pusat penyimpanan, pengelolaan, dan pemulihan data yang digunakan secara bersama oleh instansi pusat dan pemerintah daerah. Hal ini memungkinkan integrasi layanan publik yang lebih efisien dan efektif, serta mendukung interoperabilitas antar sistem pemerintahan.

Lebih lanjut, PDN mendukung transformasi digital nasional dengan menyediakan infrastruktur yang memungkinkan integrasi data dan layanan secara menyeluruh. Hal ini sejalan dengan upaya pemerintah dalam mewujudkan pelayanan publik yang berkualitas dan terpercaya melalui pemanfaatan teknologi informasi dan komunikasi. Dengan demikian, PDN menjadi fondasi penting dalam pembangunan sistem pemerintahan yang modern dan responsif terhadap kebutuhan masyarakat. Ketergantungan layanan publik terhadap infrastruktur digital pemerintah semakin meningkat seiring dengan masifnya transformasi digital dalam sektor administrasi dan pelayanan. Pemerintah saat ini banyak mengandalkan sistem digital untuk mendukung berbagai fungsi, mulai dari pengelolaan data kependudukan, layanan kesehatan, pendidikan, hingga perpajakan. Infrastruktur

[68] Ririn Aswandi,Dkk, "Perlindungan Data Dan Informasi Pribadi Melalui *Indonesia Data Protection System* (IDPS), *Jurnal Legislatif*, Vol. 3, No. 2, Juni 2020, Hlm. 182

digital seperti Pusat Data Nasional (PDN), jaringan intra-pemerintah, dan sistem aplikasi layanan publik menjadi tulang punggung bagi penyelenggaraan layanan yang cepat, efisien, dan terintegrasi. Ketika infrastruktur ini terganggu, misalnya karena serangan siber seperti ransomware atau kegagalan sistem, dampaknya sangat luas dan langsung dirasakan oleh masyarakat. Misalnya, terhentinya layanan administrasi kependudukan, gangguan dalam sistem informasi rumah sakit, atau lambatnya proses pengajuan perizinan. Hal ini menunjukkan betapa vitalnya keberadaan dan ketahanan infrastruktur digital bagi stabilitas dan keberlanjutan layanan publik. [69]

1. Kerangka Hukum Nasional Dan Internasional Pada Peretasan Data

Regulasi peretasan data nasional dan internasional, dan dibentuk untuk mengelola data pribadi yang bertujuan melindungi hak individu terkait data tersebut, serta memastikan organisasi pengelola data menjalankan kewajiban dengan transparan dan keamanan yang memadai. Pemerintah Indonesia memiliki tanggung jawab untuk menciptakan dan mengimplementasikan regulasi yang memadai dan efektif terkait data pribadi. Pemerintah harus berperan aktif dalam memberlakukan peraturan yang tepat guna, memberikan pendidikan dan kesadaran terkait hak privasi, serta melakukan pengawasan dan penegakan hukum terhadap pelanggaran privasi data. Pada tingkat internasional beberapa regulasi utama yang sering dijadikan acuan GDPR dari Uni Eropa merupakan standar global dalam perlindungan data pribadi. Memberikan hak-hak yang luas bagi pemilik data dan kewajiban bagi pengendali data untuk melindungi data secara aman.

a. Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

   Satu-satunya Pasal yang secara tegas menjamin perlindungan data pribadi setelah diproses adalah Pasal 26 Ayat 1 UU ITE, khususnya Pasal 27 hingga 37, mengatur kegiatan ilegal di bidang informasi elektronik yang tidak secara

[69] Syarifa Tommy, "Evaluasi Manjemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional", *Jurnal Ilmiah Ekonomi Dan Manajemen*, Vol. 3, Nomor 6, Juni 2025, hlm. 334-335

khusus berkaitan dengan data pribadi. Pasal-Pasal tersebut pada umumnya melarang perbuatan yang melanggar hak dan penyalahgunaan informasi elektronik dengan sengaja yang dapat merugikan orang lain, terutama pemilik informasi. Indonesia memiliki UU ITE yang juga mencakup aspek perlindungan data pribadi. Namun, menurut penulis, undang-undang ini dianggap belum cukup kuat dalam melindungi data pribadi. Pada November 2020, Indonesia mengesahkan Rancangan UU PDP untuk meningkatkan perlindungan ini. Undang-Undang tersebut mengadopsi prinsip-prinsip umum yang ditemukan dalam GDPR Uni Eropa. Uni Eropa diwakili oleh GDPR, yang mulai berlaku pada Mei 2018. GDPR memberikan kerangka kerja yang kuat untuk melindungi data pribadi warga Uni Eropa dan mengatur bagaimana data dapat dikumpulkan, diproses, dan disimpan. GDPR memberikan hak kepada individu untuk mengontrol data pribadi mereka dan memberikan sanksi yang signifikan kepada perusahaan yang melanggar peraturan ini. Perlindungan data pribadi juga dilakukan di Amerika Serikat, memiliki pendekatan yang berbeda dalam perlindungan data pribadi. Di AS, tidak ada undang-undang federal yang komprehensif mengatur perlindungan data pribadi secara umum.

Sebaliknya, berbagai undang-undang sektoral dan negara bagian mungkin berlaku. *California Consumer Privacy Act* (CCPA) adalah salah satu contoh undang-undang negara bagian yang signifikan, memberikan hak kepada penduduk California untuk mengontrol penggunaan data pribadi mereka oleh perusahaan. Secara umum, Uni Eropa memiliki salah satu kerangka perlindungan data pribadi yang paling kuat melalui GDPR, dengan penekanan pada hak individu dan sanksi yang tegas. Indonesia sedang berupaya untuk meningkatkan perlindungan data pribadinya melalui UU PDP, sementara Amerika Serikat cenderung memiliki pendekatan yang lebih terfragmentasi. [70]

[70] Kadek Rima Anggen Suari, I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia", *Jurnal Analisis Hukum,* Vol. 6, No. 1, April 2023, Hlm. 143-144

b. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Implementasi UU PDP adalah upaya pemerintah Indonesia dalam merumuskan kebijakan dan mengimplementasikan UU PDP sebagai kerangka kerja hukum yang mengatur pengumpulan, pengolahan, dan penyimpanan data pribadi. UU PDP bertujuan guna menegakkan hak warga atas keamanan swasta serta meningkatkan kesadaran masyarakat akan pentingnya melindungi informasi identitas. Bukti konkrit dari peran serta pemerintah dalam perumusan dan implementasi UU PDP adalah adopsi dan implementasi UU PDP sebagai kerangka kerja hukum yang Menyusun penghimpunan, pengolahan, serta penyimpanan data pribadi. Selain itu, pemerintah juga membentuk otoritas pengawas atau badan regulasi yang bertanggung jawab untuk mengawasi dan menegakkan UU PDP.[71]

c. Rancangan Undang-Undang Keamanan Dan Ketahanan Siber

Regulasi ini telah mengatur penyelenggaraan keamanan siber yang mencakup transaksi elektronik, aspek perlindungan data, hingga autentikasi halaman situs web, namun terbatas pada pengaturan keamanan siber dalam transaksi elektronik dan belum menyentuh pengaturan keamanan siber pada sektor lainnya. Kementerian Komunikasi dan Digital Republik Indonesia mendukung untuk pengesahan Rancangan Undang-Undang Keamanan dan Ketahanan Siber, terutama melengkapi UU ITE. Ruang lingkup pengaturan Rancangan Undang-Undang Keamanan Dan Ketahanan Siber lebih kepada bagaimana negara berupaya untuk mampu melaksanakan keamanan dan ketahanan, dan perlindungan siber di Indonesia, seperti melakukan deteksi, identifikasi, proteksi, penanggulangan, pemulihan, pemantauan, serta pengendalian pada objek-objek keamanan siber Rancangan Undang-Undang ini penting untuk segera disahkan untuk mengantisipasi dan memitigasi risiko keamanan siber agar kepentingan nasional Indonesia tetap terjaga senantiasa terlindungi. Berbagai macam kasus yang telah disebutkan setidaknya sudah

[71] Danil Erlangga Mahameru, "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia", *Jurnal Esensi Hukum*, Vol. 5, No. 2, Desember 2023, Hlm. 121

menjadi desakan untuk segera dapat memiliki aturan ketahanan siber yang mumpuni menjaga kedaulatan digital Indonesia.[72]

d. Peraturan Presiden No 39 Tahun 2019 Tentang Satu Data Indonesia

Inisiatif Satu Data Indonesia lahir sebagai upaya untuk menyediakan data yang kredibel, akuntabel dan mutakhir guna mendukung terwujudnya pembangunan serta penyelenggaraan pemerintahan yang berkualitas. Berdasarkan Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia, teridentifikasi empat komponen utama implementasi Satu Data Indonesia, yaitu 1) Perencanaan Data, 2) Pengumpulan Data, 3) Pemeriksaan Data, 4) Penyebarluasan Data. Selanjutnya, identifikasi hambatan pada masing-masing komponen tersebut dilakukan dengan memetakan hambatan yang melekat pada masing-masing komponen.[73]

Tujuan dari kebijakan Satu Data Indonesia adalah mengelola data dengan cara yang sesuai dengan standar data, interoperabilitas data, metadata, kode referensi. Data ini harus mudah diakses https://data.go.id/ dan dibagikan antara Instansi Pusat, Daerah, dan seluruh masyarakat. Satu Data Indonesia didirikan sebagai platform pengumpulan data nasional yang telah ditentukan dan juga akan mengembangkan portal yang dapat diakses melalui internet. Data yang dihasilkan Satu Data Indonesia tersedia secara gratis dan dapat dibagikan dalam format yang dapat digunakan kembali. Oleh karena itu, Satu Data Indonesia memastikan bahwa data yang dihasilkan mematuhi empat prinsip panduannya. Portal Satu Data Indonesia didirikan agar seluruh masyarakat Indonesia dapat mengakses dan mengambil manfaat dari data yang dikumpulkan dan dibagikan, serta memperoleh fakta dan informasi yang dapat dipercaya.[74]

Kerangka hukum internasional dalam peretasan data dirancang untuk melindungi hak privasi individu dalam lingkup global, terutama pada konteks

---

[72] Muhammad Arief, "Urgensi Regulasi Ketahanan Dan Keamanan Siber Dalam Undang-Undang ITE" *Jurnal Litigasi Amsir*, September 2022, Hlm.47

[73] Maulia Jayantina Islami, "Implementasi Satu Data Indonesia: Tantangan Dan *Critical Success Factors (Csfs)"*, *Jurnal Komunika,* Vol. 10, No. 1, Juni 2021, Hlm. 17

[74] Sena Putra Prabujaya, Januar Eko Aryansyah, Muhammad Firdaus Febrianyah, "Implementasi Kebijakan Satu Data Dalam Mewujudkan Open Government Data Di Provinsi Sumatera Selatan", *Jurnal Pesirah*, Vol. 4, No.2, November 2023, Hlm. 19

pertukaran hingga pemrosesan data lintas negara. Berikut beberapa regulasi utama yang berlaku secara internasional:

a. *Convention 108+*

Bagian penting dari Konvensi 108 adalah delapan prinsip dasar perlindungan data, yaitu prinsip pembatasan pengumpulan, kualitas data, spesifikasi tujuan, pembatasan penggunaan, perlindungan keamanan, keterbukaan, partisipasi individu, dan akuntabilitas. Pasal 9 dari Konvensi 108+ menyatakan secara umum setiap individu memiliki hak "untuk tidak tunduk pada keputusan yang secara signifikan mempengaruhi dirinya berdasarkan pemrosesan data secara otomatis", hak untuk mendapatkan informasi yang berkaitan dengan pemrosesan data pribadi mereka, hak untuk mendapatkan alasan yang mendasari pemrosesan data di mana hasilnya berlaku untuknya, hak untuk menolak pemrosesan data pribadinya, hak untuk mendapatkan perbaikan atau penghapusan, dan hak untuk mendapatkan pemulihan atau ganti rugi jika haknya telah dilanggar.[75]

b. International Covenant on Civil and Political Rights

Pasal 17 *International Covenant on Civil and Political Rights* (selanjutnya disebut ICCPR), mengatur mengenai hak privasi, Pasal ini memiliki bunyi yang sama dengan Pasal 12 *Universal Declaration Of Human Right*, yang menjadi pembeda antara Pasal 12 *Universal Declaration Of Human Right* dan Pasal 17 *International Covenant on Civil and Political Rights* terletak pada ayat 2 dari Pasal 17 *International Covenant on Civil and Political Rights*, Pasal 2 memberikan penegasan terkait perlindungan hak privasi. Namun di dalam *International Covenant on Civil and Political Rights* sendiri tidak menyatakan secara eksplisit bahwa data pribadi merupakan bagian dari hak privasi, namun *United Nation Human Rights Committee* (HRC) telah menyediakan pedoman detail untuk memberikan penjelasan terperinci tentang ruang lingkup dari hak privasi, penjelasan tersebut di dalam CCPR General Comment No.16 : Article 17 (*Right to Privacy*) , didalam

[75] Sherly Haristya, "*Studi Pendahuluan: Perbandingan Rancangan UU PDPDengan Konvensi Eropa 108+ Dan GDPR*", Yayasan Tifa: Jakarta, 2020, Hlm. 18

General Comment tersebut disebutkan bahwa Untuk tujuan memperoleh perlindungan yang paling efektif dari kehidupan pribadi seseorang, setiap orang harus memiliki hak untuk memastikan dalam sebuah bentuk yang dapat dipahami, dan data pribadi apa yang disimpan didalam *automatic data files*, dan untuk tujuan apa, setiap orang juga harus dapat memastikan otoritas publik atau individu atau badan swasta mana yang mungkin mengontrol data mereka, jika data itu berisi data pribadi yang salah atau telah dikumpulkan, atau diolah atau diproses bertentangan dengan hukum, maka dari itu setiap orang wajib untuk dilekatkan hak untuk meminta penghapusan atau perbaikan. Berdasarkan pernyataan di dalam *General Comment* tersebut terlihat jelas bahwa data pribadi juga merupakan bagian yang tidak terlepas dari hak privasi yang harus dilindungi dari segala pelanggaran.

c. *European Convention on Human Right*

Council of Europe yang merupakan organisasi internasional yang bersifat regional memiliki beberapa perjanjian yang mengatur mengenai perlindungan hak privasi, salah satunya adalah *European Convention on Human Right* (selanjutnya disebut ECHR). Pasal 8 ayat 1 *European Convention on Human Right* mengatur bahwa tidak ada seorangpun yang boleh diganggu urusan keluarganya, pribadinya, rumah tangganya, ataupun hubungan surat dan menyuratnya. Sementara itu Pasal 8 ayat 2 *European Convention on Human Right* mengatur mengenai penegasan perlindungan hak privasi, bahwa tidak boleh ada keterlibatan dari pihak berwenang dengan pelaksanaan dari hak ini kecuali jika berlandaskan hukum dan dibutuhkan dalam masyarakat yang demokratis untuk keperluan keamanan nasional, keamanan publik atau ekonomi yang sejahtera dari negara, untuk menghindari penyalahgunaan atau kejahatan, untuk perlindungan moral dan kesehatan, ataupun untuk perlindungan dari hak dan juga kebebasan yang dimiliki individu lain. Namun Pasal 8 *European Convention on Human Right* merupakan dasar terbentuknya konvensi lain yang mengatur secara detail mengenai data pribadi, konvensi tersebut adalah *The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* yang ditandatangani oleh perwakilan negara

anggota tahun 1981 dan diterapkan tahun 1985 setelah ratifikasi dari sejumlah negara sebagaimana dipersyaratkan.[76]

d. *Council of Europe Convention for the Protection of Individuals With Regard to Processing of Personal Data*

Tujuan Konvensi ini adalah untuk melindungi setiap orang di wilayah *Council of Europe*, terlepas dari kebangsaan dan tempat tinggal mereka, untuk menghormati hak dan kebebasan mendasar mereka, terutama hak atas privasi, dalam pemrosesan otomatis data pribadi yang terkait dengan ini. Pasal 2 CETS No.108 menyatakan bahwa data pribadi adalah segala informasi yang memiliki keterkaitan dengan pengenalan seseorang. CETS No.108 juga mengatur mengenai prinsip prinsip perlindungan data pribadi yang diatur didalam bagian kedua dalam konvensi ini. Bagian ketiga konvensi mengatur mengenai pengiriman lintas batas negara. Selain Council of Europe, organisasi internasional lainnya dalam kawasan eropa yakin European Union juga memiliki instrumen hukum internasional yang mengatur mengenai perlindungan hak privasi dan perlindungan data pribadi yaitu *Charter of Fundamental Right of the European Union* (Selanjutnya disebut CFREU).

e. *Charter of Fundamental Right of the European Union*

Charter of Fundamental Right of the European Union (CFREU) mengatur hak privasi dan data pribadi di dalam 2 Pasal yang berbeda, dimana hak privasi diatur dalam Pasal 7 dan perlindungan data pribadi dalam Pasal 8. Pasal 7 menyebutkan bahwa setiap orang mempunyai hak agar dihormati kehidupan pribadi, rumah, dan komunikasinya. Sementara itu Pasal 8 ayat 1 menyatakan bahwa setiap orang memiliki hak atas perlindungan data pribadi, ayat 2 menyatakan bahwa data tersebut harus diproses secara adil, untuk tujuan khusus, atas persetujuan subjek data, sesuai dengan aturan hukum. Uni Eropa memiliki pengaturan yang lebih spesifik berkenaan dengan perlindungan data pribadi yaitu, *European Union General Data Protection Regulation* (selanjutnya disebut GDPR).

[76] Eliezer Nathaniel, "Aspek Perlindungan Hukum Internasional Data Pribadi Pengguna Layanan Jejaring Sosial Dan Kewajiban Korporasi Penyedia Layanan", *Jurnal Kertha Desa*, Vol.9. No. 7, Hlm. 92

f. European Union General Data Protection Regulation

General Data Protection Regulation (GDPR) berlaku terhadap pengontrol data dan pemroses data yang didirikan di kawasan Uni Eropa atau yang berada diluar kawasan namun memiliki target terhadap individu yang berada dalam kawasan Uni eropa, sebagai contoh, Facebook dimana penggunanya banyak yang merupakan penduduk negara-negara anggota dari Uni Eropa. GDPR berlaku untuk pemrosesan data pribadi. Definisi data pribadi berdasarkan instrument tersebut yaitu informasi apa pun yang terkait atau terkait dengan individu yang mengidentifikasi atau mengidentifikasi seseorang, termasuk data seperti alamat IP, email, atau nomor telepon.

Selain itu, GDPR memberikan perlindungan tambahan untuk pemrosesan kategori data pribadi tertentu, termasuk pengungkapan asal ras atau etnis seseorang, opini politik, agama, keyakinan filosofis, keanggotaan serikat pekerja, genetika, teknologi biometrik, dan data yang terkait dengan kesehatan pribadi. Data pribadi dan orientasi seksual. Namun, negara-negara Uni Eropa dapat mengajukan pembatasan atau pembatasan pemrosesan data genetik dan biometrik atau data kesehatan. osesan data genetik dan biometrik atau data kesehatan. GDPR juga mengatur mengenai prinsip-prinsip fundamental mengenai pemrosesan data pribadi, yaitu:

1) Diproses dengan adil, transparan, dan sesuai aturan hukum
2) Sesuai dengan tujuan tertentu
3) Akurat, memadai, relevan, dan berhubungan dengan tujuan pemrosesan
4) Batasan penyimpanan tertentu, dimana data tidak diperbolehkan untuk disimpan dalam jangka waktu yang lebih lama dari yang dibutuhkan untuk tujuan pengumpulan
5) Integritas, rahasia, dan jaminan keamanan
6) Akuntabilitas, pengendali harus bertanggung jawab untuk dapat menunjukkan kepatuhan seperti yang disebutkan sebelumnya.

Selain tentang pemrosesan *General Data Protection Regulation* juga mengatur tentang hak-hak dari subjek data, antara lain:

1) Hak transparansi
2) Hak atas informasi
3) Hak akses terhadap data pribadi
4) Hak ratifikasi
5) Hak penghapusan data pribadi
6) Hak atas keterbukaan data pribadi
7) Hak untuk menolak dan keputusan otomatis.
8) Pembatasan

Negara pihak dalam GDPR mewajibkan untuk menyediakan suatu otoritas independen untuk bertanggungjawab atas pemantauan regulasi. Otoritas pengawas berkewajiban untuk berkontribusi secara konsisten dan harus bekerjasama dengan otoritas lainnya

g. OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data

Instrument ini merupakan pernyataan pertama mengenai perlindungan data, yang mengandung muatan mengenai prinsip perlindungan dan standar minimum bagi negara anggota, namun instrumen ini bukan merupakan instrumen hukum yang bersifat hard law sehingga tidak memiliki kekuatan mengikat secara hukum, instrument ini hanya berupa rekomendasi atau guidelines bagi negara anggota dalam OECD. Mengingat bahwa panduan ini tidak mengikat secara hukum, dan mengingat OECD hanya diakui sebagai organisasi internasional oleh negara negara anggotanya, berdasarkan Pasal 38(1) Statuta Mahkamah Internasional, perlindungan data pribadi OECD diklasifikasikan sebagai general principle of law.[77]

2. Struktur Organisasi Kelembagaan Kementerian Komunikasi dan Digital Dan Badan Siber Dan Sandi Negara

Penguatan tata kelola ekosistem pada Pusat Data Nasional dalam transformasi digital pemerintah bahwa penguatan struktur organisasi dari Kementerian Komunikasi dan Digital dan badan siber dan sandi negara berperan

[77] *Ibid,* Hlm. 98

penting dalam keamanan siber Pusat Data Nasional agar dapat lebih siaga dalam menghadapi mitigasi serangan siber. Dengan adanya permasalahan terhadap penanganan *cyber security* dalam kerangka pertahanan negara yang masih bersifat sektoral dan belum terkoordinasi serta belum terpadu, pada akhirnya, mendorong pemerintah untuk membentuk Badan Siber dan Sandi Negara pada 19 Mei 2017 melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. Beberapa lembaga lain yang memiliki kepentingan dalam area pertahanan keamanan nasional termasuk lingkup siber disinergikan di bawah Badan Siber Dan Sandi Negara ini. Kementerian Pertahanan, TNI, Polri, Badan Intelijen Negara, Kementerian Komunikasi Dan Digital, Lembaga Sandi Negara, dan berbagai instansi terkait lainnya adalah Lembaga-lembaga pemerintah yang perlu disinergikan untuk menangkis, menangkal, dan mencegah serangan *cyber* baik yang dilakukan dalam negeri maupun luar negeri.[78]

Dalam perspektif Nasional, sebuah negara, instansi pemerintah, organisasi bisnis untuk menjaga kepentingan, dan aset pentingnya keberadaan Pusat Data menjadi penting. Terselenggaranya layanan sistem informasi, akses informasi publik sampai keperluan tata kelola pemerintahan akan melalui, disimpan dan dikelola pada Pusat Data. Nilai aset data dan informasi yang dikelola Pusat Data berorientasi jangka panjang baik secara penyimpanan dan penggunaannya di masa mendatang. Negara dapat hadir dalam pengelolaan aset ini dengan menyediakan Pusat Data Nasional yang dapat digunakan untuk kepentingan Pemerintahan, Militer, dan Publik. Pengelolaan dapat dilakukan secara terbuka, terbatas dan tertutup tergantung dari subjek/objek Pusat Datanya. Kumpulan server dan sistem penyimpanan data membutuhkan fasilitas untuk menampung semua sumber daya yang dimiliki. Fasilitas tersebut harus memenuhi kondisi server yang memungkinkan untuk melakukan pengaturan sumber daya, pengaturan udara serta memiliki sistem pengamanan fisik. Fasilitas yang menjadi pusat penampungan data (data center) ini memiliki beberapa kriteria khusus dalam perancangannya, antara lain:

[78] Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara", *Jurnal Politica,* Vol.10. No.2, Desember 2019, Hlm 121

a. *Availability*, Data center mampu menjalankan operasi secara berkelanjutan dan terus menerus dalam kondisi apapun.
b. *Scalability* dan *Flexibility*, Data Center mampu beradaptasi dengan pertambahan kebutuhan atau teknologi baru tanpa merubah substansi data center secara keseluruhan.
c. *Security*, Data Center mampu melindungi aset data yang tersimpan pada server secara fisik maupun non-fisik.[79]

Asas kehati-hatian dalam konteks perlindungan data pribadi mengacu pada tindakan proaktif dan pencegahan yang diambil oleh pemerintah untuk memastikan bahwa data pribadi dikelola dan dilindungi dengan cara yang aman dan sesuai dengan peraturan perundang undangan yang ada. Hal ini mencakup berbagai tindakan preventif untuk mencegah pelanggaran data dan meminimalkan risiko penyalahgunaan data pribadi. Dalam UU PDP menetapkan adanya otoritas perlindungan data yang bertugas mengawasi kepatuhan terhadap undang-undang tersebut. Tantangan lainnya ke depan dalam pengembangan kebijakan *cyber security* adalah sifat dari ancaman siber yang multidimensional membuat penanganannya tidak hanya menjadi tanggung jawab dari TNI dan/atau Polri. Kementerian Pertahanan maupun Kementerian Komunikasi dan Digital.

Menurut Sjafrie Sjamsoeddin, ancaman siber termasuk dalam ancaman asimetris yang penanganannya membutuhkan pendekatan komprehensif. Karena sifatnya multidimensional, membuat *cybersecurity* tidak dan bukan merupakan urusan satu kementerian saja, tetapi juga urusan berbagai kementerian lainnya. Karena itu diperlukan kebijakan *cybersecurity* atau *cyber defence* yang dalam implementasinya membutuhkan badan koordinasi. Dari bagan pengorganisasian dan kelembagaan penanganan *cyber security* secara nasional tersebut dapat diketahui bahwa penanganan *cyber security* harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait yaitu intelijen, penegak hukum, pertahanan dan keamanan baik itu Kementerian Pertahanan maupun TNI serta pemerintah

[79] Mardhani Riasetiawan, 2020, *Pusat Data Untuk Pemerintahan*, Https://Cloud.Wg.Ugm.Ac.Id/Wp-Content/Uploads/Sites/1288/2020/11/Pusat-Data-Untuk-Pemerintahan.Pdf , Dikutip Tanggal 08 Agustus 2024, Hlm. 5-6

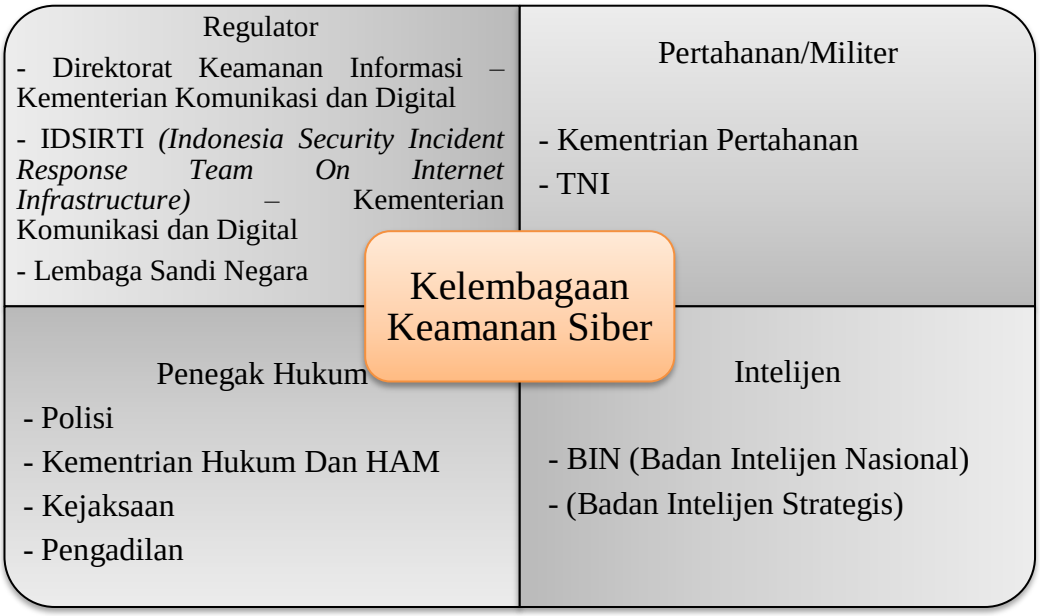
sebagai regulator yang dalam hal ini diwakili oleh Kementerian Komunikasi Dan Digital dan ISSIRTI serta Lembaga Sandi Negara.[80]

Kebijakan *cyber security* yang telah dijalankan di Indonesia telah diinisiasi sejak tahun 2007 dengan dibentuknya *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi Dan Digital untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII di antaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkait di dalam maupun luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem database sistem ID-SIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.[81]

[80] Handrini Ardiyanti, "*Cybersecurity* Dan Tantangan Pengembangannya Di Indonesia", *Jurnal Politica,* Vol. 5, No.1, Juni 2014, Hlm. 105

[81] *Ibid,* Hlm. 108

Bagan Organisasi Dan Kelembagaan *Cyber Security* Nasional



Otoritas ini memiliki wewenang untuk melakukan inspeksi, menyelidiki pelanggaran, dan memberikan sanksi jika diperlukan dan apabila ditemukan pelanggaran terhadap ketentuan undang-undang, maka pengendali data dapat dikenai sanksi administratif berupa denda, serta sanksi pidana bagi pelanggaran yang lebih serius, seperti penyalahgunaan data pribadi. Pemerintah dan lembaga terkait harus aktif melakukan edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi dan bagaimana cara melindungi data mereka sendiri. Oleh karena itu, seluruh stakeholder, perlu mendapatkan pelatihan yang memadai tentang asas kehati-hatian dan praktik terbaik dalam pengelolaan data pribadi. Sehingga Indonesia perlu mengadopsi standar internasional dalam perlindungan data pribadi untuk memastikan bahwa perlindungan data di Indonesia sejajar dengan praktik terbaik global. Karena dengan adanya kerjasama dengan negara lain dalam berbagi informasi dan teknologi terkait

keamanan data dapat membantu meningkatkan perlindungan data pribadi di Indonesia sehingga kejadian peretasan yang yang baru-baru ini tidak terjadi. [82]

3. Upaya Perlindungan Negara Terhadap Ancaman *Cyber Security* Dari Segi Hukum

Satu tantangan besar dalam mempertahankan dan menjaga kerahasiaan, integritas, dan ketersediaan informasi serta Sistem Elektronik yang strategis ialah bahwa selalu ada kemungkinan perang siber (*cyber war*) tersebut bukanlah perang yang kasat mata, tetapi perang laten. Adanya serangan siber (*cyber attack*) yang tidak dilangsungkan atas nama negara tertentu. Pembentukan peraturan perundang-undangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya. Terdapat tiga indikator dalam aspek hukum yaitu keberadaan Undang-Undang Kejahatan Siber, Undang-Undang Keamanan Siber, dan penyelenggaraan keamanan siber bagi penyelenggara hukum. Dari ketiga indikator tersebut, dalam rangka pemenuhan aspek hukum terkait penyelenggaraan keamanan siber di Indonesia, pada tahun 2019 Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber telah diinisiasi oleh Dewan Perwakilan Rakyat yang kemudian sudah diserahkan kepada pemerintah.[83]

Saat ini kebijakan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktivitas kehidupan manusia oleh

---

[82] Andri Pranata,Dkk, "Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan UU PDPDi Era Digital 5.0", *Journal Of Law And Nation*, Vol 3, No.3, Agustus 2024, Hlm. 726

[83] Satya Muhammad Sutra, Agus Haryanto, "Upaya Peningkatan Siber Indonesia Oleh Badan Siber Dan Sandi Negara Tahun 2017-2020", *Jurnal Global Political Studies*, Vol. 7, No. 1, April 2023, Hlm.63

karena itu dibutuhkan pengaturan secara khusus dengan dibentuknya suatu undang-undang yang dapat menanggulangi kejahatan terhadap teknologi informasi. Pembentukan peraturan perundang-undangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

Sebelum diundangkannya UU ITE yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan *cybercrime* tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan- perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-undang. Untuk meningkatkan upaya penanggulangan kejahatan siber atau *cyber crime* yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan cyber dan cara penanganannya kepada satuan di kewilayahan (Polda).

Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan *cybercrime*. Selain upaya dari kepolisian, kesadaran hukum masyarakat sangat diperlukan dalam berteknologi dan rendahnya kesadaran hukum para netter menjadikan penegakan hukum terhadap *cybercrime* tidak berjalan optimal.[84] Mengingat perlunya penyelarasan strategi *cyber security* dengan transformasi digital menjadi solusi keamanan berlapis. Di lapisan pertama adalah unit kerja, baik tim teknologi informasi maupun tim bisnis. *Security requirement, security awareness*, kemampuan-kemampuan mendesain solusi yang secure sambil mendeliver pengalaman yang menyenangkan, Kemudian di lapisan kedua ada tim manajemen risiko dan kepatuhan. Tim ini harus memiliki visibilitas risiko keamanan siber yang komprehensif dan terbarukan untuk

[84] Utin Indah Permata Sari, "Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia", *Jurnal Hukum Mimbar*, Vol. 2, No. 1 Tahun 2021, Hlm. 15

kemudian dibahas Bersama. Di lapis tiga adalah tim audit, untuk melihat apakah kontrol yang terkait *cyber security* ini sudah memadai atau belum, apakah perlu perbaikan.

Tim audit ini harus dibekali dengan kapabilitas dan pengetahuan yang memadai untuk menghadapi risiko *cyber security* masa kini. Yaitu kemampuan tentang bagaimana cara mengaudit keamanan *cloud, agile development*, dan lain-lain. Masalah *cyber security* sangat kompleks, untuk itu memerlukan pendekatan multidimensional. Karenanya, untuk meningkatkan tata kelola *cyber security*, pelaksanaan prinsip multi pihak (multi stakeholderism) menjadi sangat penting. Tanpa adanya kerja sama dan kolaborasi di kalangan pemangku kepentingan (dari lembaga layanan publik hingga sektor swasta, akademisi dan masyarakat sipil), problem solving isu terkait *cyber security* akan terus menjadi satu dimensi dan tidak lengkap. Diperlukan sebuah mekanisme inklusif yang dapat mengesahkan keputusan sekaligus reflektif dan responsif terhadap kepentingan nasional dan populasi yang terdampak. Kerjasama internasional sangat diperlukan, terkait dengan pengembangan dan penguatan kapasitas kemampuan *cyber security* baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan SDM dalam bidang *cyber security* baik bilateral antar dua negara maupun regional maupun internasional. Peningkatan kerja sama teknologi informasi dan *cyber security* selain itu juga diharapkan mampu membuka peluang bagi pengembangan industri media baru terkait dengan teknologi informasi di Indonesia sebagai salah satu bagian dari pengembangan industri strategis Nasional.[85]

Menurut O. Notohamidjojo, pengertian hukum merupakan peraturan yang tertulis maupun tidak tertulis yang pada umumnya bersifat memaksa perilaku masyarakat dalam bermasyarakat. Hukum dapat digunakan dalam mewujudkan perlindungan yang tentunya tidak hanya bersifat adaptif dan fleksibel, namun juga bersifat antisipatif dan prediktif. Perlindungan hukum yang dilakukan pemerintah ditujukkan untuk mencegah sebelum terjadinya pelanggaran. Pemberian sanksi berupa denda, kurungan, dan hukuman tambahan yang

[85] Eko Budi, Dkk, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0", *Jurnal Prosiding Senastindo AAU*, Vol. 3, Tahun 2021, Hlm. 233

dijatuhi atas permasalahan yang timbul karena dilarangnya suatu peraturan. Sedangkan menurut pendapat M. Isnaeni, suatu perlindungan hukum dianalisis dari sumbernya dibagi menjadi 2 (dua) yaitu perlindungan hukum eksternal dan perlindungan hukum internal. Hakikat perlindungan hukum internal, pada dasarnya perlindungan hukum yang dimaksud untuk diolah-olah oleh pihak yang membuat suatu perjanjian, dimana saat menyusun Pasal-Pasal dalam perjanjian, para pihak menginginkan agar kepentingannya diakomodir.[86] Perlindungan data pribadi sebagai bagian dari identitas individu merupakan isu yang penting khususnya di Indonesia. Di Indonesia UU PDP yang bertujuan untuk melindungi data pribadi, mencerminkan komitmen negara untuk menyelaraskan diri dengan standar internasional.

Kerangka kerja perlindungan data di Indonesia, meskipun terus berkembang, masih tertinggal dari standar internasional seperti Perlindungan Data Umum atau GDPR Uni Eropa. GDPR terkenal dengan pendekatannya yang komprehensif terhadap perlindungan data, menawarkan hak-hak yang kuat pada subjek data, termasuk hak untuk mengakses, memperbaiki, dan menghapus data pribadi, di samping kewajiban yang ketat bagi pengontrol dan pengolah data untuk memastikan transparansi dan akuntabilitas dalam penanganan data. Penelitian menunjukkan bahwa undang-undang perlindungan data di Indonesia saat ini belum sepenuhnya sejalan dengan persyaratan ketat GDPR. Kurangnya otoritas perlindungan data yang terpusat di Indonesia menghambat implementasi dan penegakan hukum perlindungan data yang efektif, sebuah fitur yang sudah mapan di bawah kerangka kerja GDPR.

Kerangka hukum Indonesia tidak memiliki beberapa ketentuan utama yang ditemukan dalam GDPR. Sebagai contoh, konsep probabilitas data, yang memungkinkan individu untuk mentransfer data mereka dari satu penyedia layanan ke penyedia layanan lainnya, tidak secara eksplisit dibahas dalam hukum Indonesia. Selain itu, penekanan GDPR pada persetujuan eksplisit dan hak untuk dilupakan tidak sepenuhnya tercermin dalam undang-undang perlindungan data di Indonesia. Kurangnya otoritas perlindungan data yang

[86] Jonathan Elkana Soritua Aruan, "Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi", *Jurnal Globalisasi Hukum*, Vol.1, No.1, April 2024, Hlm. 5

terpusat di Indonesia, menghambat implementasi dan penegakan hukum perlindungan data yang efektif, sebuah fitur yang sudah mapan dibawah kerangka kerja GDPR.

IV. PENUTUP

A. Kesimpulan

1. Dalam hal ini Pusat Data Nasional menjadi bukti bahwa masih adanya celah antara kebijakan dan implementasi di lapangan, mulai dari segi kesiapan teknologi, sumber daya, hingga kebijakan yang belum efektif. Dalam budaya hukum di Indonesia yang berkenaan dengan kesadaran, kepatuhan, dan perilaku dari masyarakat hingga penegak hukum yang mengimplementasikan kebijakan serta regulasi yang ada, dalam hal ini masih banyak instansi pemerintahan yang lalai pentingnya keamanan data, masih rendahnya kepatuhan terhadap regulasi yang ada sehingga masyarakat juga belum menyadari bahwa pentingnya keamanan data pribadi. Jika struktur hukum sendiri tidak ditemukan permasalahan yang signifikan namun pada sisi budaya hukum dan penegakan hukum ditemukan celah yang mengakibatkan tidak efektifnya regulasi tersebut. Pada penelitian ini didapatkan kebocoran data diakibatkan oleh fasilitas yang berlum sesuai standar internasional dalam keamanan data dan sumber daya manusia yang belum cukup handal dalam mitigasi kebocoran data sehingga diperlukan upaya penegakan hukum yang menimbulkan efek jera.

2. Strategi yang dilakukan oleh lembaga di Indonesa dalam menanggulangi serta meminimalisir risiko kebocoran data secara represif insiden kebocoran data di Pusat Data Nasional menjadi tolok ukur pemerintah bahwa perlunya penguatan regulasi dan kebijakan yang ada dan disertai dengan dukungan dari masyarakat. Melihat Pasal 15 ayat (1) UU ITE bahwa, setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik. Dari Pasal tersebut menandakan bahwa pusat data nasional yang dikelola oleh Kementerian Komunikasi dan Digital wajib menjamin keamanan sistem elektronik yang digunakan untuk mencegah kebocoran data. Kemudian pada Pasal 58 ayat (2) UU PDP bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh Lembaga, ini

yang menjadi dasar bahwa perlu adanya Lembaga pengawas yang bertanggung jawab sebagai pengawas pusat data nasional.

Sedangkan secara preventif perlunya penegasan tanggung jawab hukum pada setiap pelaku dalam struktur UU PDP jika terjadi insiden kebocoran data akibat kelalaian atau pelanggaran standar operasional. Untuk itu pemerintah berkolaborasi bersama stakeholder lainnya untuk menjaga ruang siber dengan memperkuat ekosistem keamanan siber nasional sehingga menciptakan perencanaan strategis khususnya bidang keamanan siber. Pengembangan teknologi dengan sistem deteksi dini melalui monitoring sangat menunjang dalam penjagaan ruang siber. Kebijakan yang kuat juga sangat penting dalam upaya memperkuat keamanan data. Kebijakan yang jelas mengenai penanganan insiden siber, termasuk prosedur tanggap darurat dan pelaporan insiden, juga harus dapat ditangani dengan cepat dan efisien. Pusat Data Nasional perlu memastikan bahwa semua pegawainya memiliki pemahaman yang kuat tentang praktik keamanan siber dan dilatih untuk mengenali dan merespon ancaman potensial.

B. Saran

Pembentukan otoritas perlindungan data independen yang sesuai tertuang dalam UU PDP yang perlu diberi kewenangan secara jelas dan terstruktur. Penyusunan seperti ini dirasa perlu untuk memperjelas kedudukan serta tanggung jawab dari struktur lembaga/instansi yang berkenaan langsung dengan keamanan data di Indonesia, seperti kedudukan Badan Siber dan Sandi Negara, Kementerian Komunikasi dan Digital, serta Kepolisian Republik Indonesia dalam implementator penegakan hukum. Penandatanganan pakta integritas oleh *Data Protection Officer* dapat menjadi salah satu strategi dan upaya dalam pengelolaan data informasi nasional sehingga apabila terjadinya insiden kebocoran data, hukum dapat ditegakkan menurut undang-undang. Serta kolaborasi antar lembaga pemerintah yang terstruktur sesuai prosedur yang dicantumkan pada Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia sebagai regulasi pendukung UU PDP.

DAFTAR PUSTAKA

A. Buku

Ashshofa, Burhan, 2010, *Metode Penelitian Hukum*, Jakarta.

Djafar, Wahyudi, 2016, *Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*, Jakarta.

Haristya, Sherly, 2020, Studi Pendahuluan: *Perbandingan Rancangan Undang-Undang Perlindungan Data Pribadi dengan Konvensi Eropa 108+ dan GDPR*, Jakarta.

Karo Karo, Rizky P.P, 2020, *Pengaturan Perlindungan Data Pribadi Di Indonesia,* Bandung.

Martien, Dhoni, 2023, *Perlindungan Hukum Data Pribadi*, Makassar.

Miles, Matthew B, A. Michael Huberman, 2001, *Analisis Data Kualitatif*, Jakarta.

Salako, Maskun Wiwik Meilarati, 2017, *Aspek Hukum Penipuan Berbasis Internet*, Bandung.

Sari, Ika Yusnita, dkk, 2020, *Keamanan Data Dan Informasi*, Kisaran.

Soemitro, Ronny Hanitijo, 1998, *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta.

Timotus, Kris H., 2017, *Pengantar Metodologi Penelitian*, Yogyakarta.

B. Jurnal

Althafferani F Nasution, dkk, "Pengaruh Tindak Pidana Korupsi Mega Proyek BTS (Base Transceiver Station) Oleh Kementerian Komunikasi dan Digital Terhadap Tingkat Kepercayaan Mahasiswa Ilmu Politik UPN Veteran Jakarta", *Jurnal Independen*, Vol.5, No.1, April 2024

Alza Gabriel, "Perlindungan Hukum Atas Data Pribadi Dalam Kasus Kebocoran Data Pusat Data Nasional Dalam Perspektif Hukum Pidana", *Jurnal Hukum dan Pancasila*, Vol. 3, No 12, Juni, 2024

Anak Agung Putu Wiwik Sugiantri, dkk, "Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masayarakat Dari Pusat Data Nasional Indonesia", *Jurnal Hukum Saraswati,* Vol. 6, Nomor 2, 2024

Andi Rania Risya, "Kajian Teoritis Implikasi *The United Nations Convention Against Cybercrime* Terhadap Pengaturan Tindakan Pidana Siber Indonesia", *Jurnal Ikraith Humaniora,* Vol.9, Nomor 2, Juli 2025

Andrew Ardiyanto Dachlan, "Pertanggungjawaban Hukum Pemerintah Dalam kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional", *Jurnal Hukum Samudra Keadilan,* Vol. 20, Nomor 1, Januari-Juni 2025

Andri Pranata, dkk, "Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan UU PDP di Era Digital 5.0", *Journal of Law And Nation,* Vol.3, No.3, Agustus 2024

Anna S. Wahongan, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2026 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik", *Jurnal Lex Privatum,* Vol. 10, Nomor 1, Januari 2022

Ardimansyah, dkk, "Tantangan Penanganan Ancaman Siber Dalam Menyongsong Pemilihan Umum 2024", *Jurnal Budget Issue Brief,* Vol. 02, 16 September 2022

Arief Bakhtiar Darmawan, dkk, "Kedaulatan Negara Dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook Dan Google", *Jurnal Hubungan Internasional,* Vol. 16, No. 1, Januari-Juni 2023

Bayu Adinegoro, "Kebijakan Satu Data Indonesia: Sebuah Antitesis Semangat Keterbukaan Dan Informasi Publik", *Jurnal Kebijakan,* Vol. 16, Nomor 1, Januari 2025

Bisri Fadil Hasan, "Perlindungan Hukum Data Pribadi Terhadap Konsumen Pinjaman Berbasis Online", *Skripsi,* Univeritas Syarif Hidayatullah Jakarta, 2023

Aryojati Ardipandanto, "Lemahnya Pengamanan Pusat Data Nasional Terhadap Serangan Siber", *Jurnal Info Singkat*, Vol. 14, No. 13, Juli 2024

Danil Erlangga Mahameru, "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia", *Jurnal Esensi Hukum*, Vol. 5, No. 2, Desember 2023

Dayu Medina, "Perlindungan Sumber Daya Genetik Dan Pengetahuan Tradisional Dalam Kerangka WIPO", *Jurnal Das Sollen*, Vol. 01, Nomor 1, Juni 2024

Dede Suprayitno, dkk, "Kebijakan Keamanan Siber Dan Kedaulatan Data: Suatu Kunci Dalam Mewujudkan Digitalisasi Pemilu di Indonesia", *Jurnal Administrasi Publik*, Vol. 10, No. 1, April 2024

Dewi Triwahyuni, Tine Agustin, "Strategi Keamanan Cyber Amerika Serikat", *Jurnal Ilmu Politik Dan Komunikasi*, Vol 6, No 1, Juni 2016

Eliezer Nathaniel, "Aspek Perlindungan Hukum Internasional Data Pribadi Pengguna Layanan Jejaring Sosial Dan Kewajiban Korporasi Penyedia Layanan", *Jurnal Kertha Desa*, Vol.9. No. 7

Eko Budi, dkk, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0", *Jurnal Prosiding Senastindo AAU*, Vol. 3, tahun 2021

Endison Ravlindo, Ariawan Gunadi, "Perlindungan Hukum Terhadap Data Kesehatan Melalui Pengesahan Rancangan UU PDP", *Jurnal Hukum Adiguna*, Vol 4, Nomor 2, Desember 2021

Esther Hanaya, "Perlindungan Data Pribadi Di Era Digital Dalam Perspektif Perbandingan Hukum, *Jurnal Bevinding*, Vol. 1, No. 9, 2023

Fauzi Anshari Sibarani, Sekar Ayu Diningrum, "Regulasi Perlindungan Data Pribadi Terhadap Catatan Kejahatan Dalam Perspektif Hak Asasi Manusia", *Jurnal Sanksi*, Vol 3, No 1 2021

Fikri Irfan Adristi, Erika Ramadhani, "Analisis Dampak Kebocoran Data Pusat Data Nasional Smeentara 2 Surbaya: Pendekatan Matriks Budaya Kemanan Siber Dan Dimensi Budaya Nasional Hofstede". *Jurnal Selekta Manajemen*, Vol.02, No. 06, 2024

Guswan Hakim, Jabalnur, dkk, "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia", *Haluleo Legal Research,* Vol 5, No.2, Agustus 2023

Handrini Ardiyanti, "Cyber Security Dan Tantangan Pengembangannya Di Indonesia", *Jurnal Politica,* Vol, 5, No 1, Juni 2014

Hani Puspita Sari, "Efektivitas Hukum Perlindungan Data Pribadi Terhadap Kejahatan Siber Di Indonesia*", Jurnal Media Akademik,* Vol. 2, No. 11, November 2024

Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara", *Jurnal Politica,* Vol.10. No.2, Desember 2019

Imanuel Toding Bua, Nur Isdah Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024", *Jurnal Hukum, Kebijakan Publik, dan Pemerintahan,* Vol.2, No.2, Mei 2025

Jonathan Elkana Soritua Aruan, "Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi", *Jurnal Globalisasi Hukum,* Vol.1, No.1, April 2024

Jonathan Riko Mono, Lewiandy, "Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi Dalam Insiden Serangan SIber Pusat Data Nasional", *Jurnal Ilmu Hukum, Humaniora, dan Politik*, Vol. 5, No. 1, November 2024

Kadek Rima Anggen Suari, I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia", *Jurnal Analisis Hukum*, Vol. 6, No. 1, April 2023

Maulia Jayantina Islami, "Implementasi Satu Data Indonesia: Tantangan Dan Critical Success Factors (CSFs)", *Jurnal Komunika,* Vol. 10, No. 1, Juni 2021

Muhammad Arief, "Urgensi Regulasi Ketahanan Dan Keamanan Siber Dalam Undang-Undang ITE" *Jurnal Litigasi Amsir,* September 2022

Muhammad Asthi Seta Ari Yuwana, "Analisa Dampak Kebocoran Data Pusat Data Nasional Dalam Perspektif HAM", *Jurnal Wicarana*, Vol. 4, Nomor 1, Maret 2025

M. Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)", *Jurnal Politica*, Vol. 13 No. 2 Nov 2022

Muh Rifqy Hidayatullah Arham, M. Chaerul Risal, "Perlindungan Data Pribadi Bagi Pengguna Media Sosial", *Jurnal Al-Tasyriiyah*, Vol. 3, No. 2, 2023

Nabiha Khansa Rusyada, "Perlindungan Hukum Terhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022", *Jurnal Hukum DesentralisasiI*, Vol.2, No.3, Agustus 2025

Rafli Al Ihsan, Binastya Anggara Sekti, "Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia", Artikel: Prosiding Seminar Nasional Sistem Informasi Dan teknologi, Vol. 8, 2024

Rini Retno Winarni, "Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana Cyber Crime", *Jurnal Hukum Dan Dinamika Masyarakat*, Vol.14, No.1 Oktober 2016

Ririn Aswandi, dkk, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS), *Jurnal Legislatif*, Vol. 3, No. 2, Juni 2020

Riyantika Pratiwi, Tri Novita Sari Manihuruk, Irwan Harapah, "Tinjauan Yuridis Perlindungan Data Pribadi Dalam Transaksi E-Commerce", *Jurnal Pagaruyuang*, Vol 7, No 2, Januari 2024

Ruben Coda Sifiq Indonesian, dkk, "Analisis Privasi Data Pengguna Dalam Instansi BPJS Kesehatan", Prosiding Seminar Sitasi, UPN Veteran Jawa Timur, 13 November 2021

Satya Muhammad Sutra, Agus Haryanto, "Upaya Peningkatan Siber Indonesia Oleh Badan Siber Dan Sandi Negara Tahun 2017-2020", *Jurnal Global Political Studies*, Vol. 7, No. 1, April 2023

Sena Putra Prabujaya, Januar Eko Aryansyah, Muhammad Firdaus Febrianyah, "Implementasi Kebijakan Satu Data Dalam Mewujudkan Open Government Data Di Provinsi Sumatera Selatan", *Jurnal Pesirah*, Vol. 4, No.2, November 2023

Siti Yuniarti, Erni Herawati, "Analisis Hukum Kedaulatan Digital Indonesia", *Jurnal Pandecta*, Vol.15, No.2, Desember 2020

Syafira Agata Ramadhani, "Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa", *Jurnal Hukum Lex Generalis*, Vol. 3, No. 1, Januari 2022

Syarifa Tommy, "Evaluasi Manjemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional", *Jurnal Ilmiah Ekonomi Dan Manajemen*, Vol. 3, Nomor 6, Juni 2025

Utin Indah Permata Sari, "Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia", *Jurnal Hukum Mimbar*, Vol. 2, No. 1 tahun 2021

Verina Dwi Muryani, Sidi Ahyar Wiraguna, "Efektivitas Undang-Undang Perlindungan Data Pribadi Dalam Menjawab Tantangan Keamanan Siber Di Indonesia", *Jurnal Hukum dan Kewarganegaraan*, Vol. 12, No. 3, Mei 2025

Wahyudi Djafar, "Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia", Lembaga Studi Dan Advokasi Masyarakat, 2016

Wisnu Handi Prabowo, Satriya Wibawa, Fuad Azmi, "Perlindungan Data Personal Siber di Indonesia", *Jurnal Relasi Internasional Padjajaran*, Vol. 1 No. 3 Januari 2020

Yustika Citra, dkk, "Strategi Penanganan Keamanan Siber Di Indonesia", *Jurnal Review Pendidikan Dan Pengajaran*, Vol 6, No 2, 2023

C. Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia 1945

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang

Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014

tentang Pedoman Pertahanan Siber, Berita Negara Republik Indonesia Tahun 2014 Nomor 1712

Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu

Data Indonesia, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang

Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang

Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905

D. Website

Aprillio Akbar, 27 Juni 2024, Pusat Data Nasional Lumpuh Akibat Ransomeware, Mengapa Instansi Pemerintah Masih Rentan Terkena Serangan https://www.bbc.com/indonesia/articles/cxee2985jrvo , diakses pada 8 Juni 2025

Awan Pintar, https://map.awanpintar.id/ , diakses tanggal 19 Februari 2025

Benedicta Prima, 1 Juli 2024, Pusat Data Nasional Bocor: Apa Saja Datanya, https://momsmoney.id.kontan.co.id/news/pusat-data-nasional-bocor-apa-saja-datanya , diakses 8 Juli 2025

Chella Defa Anjelina, Mahardini Nur Afifah, 01 januari 2024, Menkominfo Sebut Anggaran BSSN Terbatas, Benarkah? Ini Besarnya 5 Tahun Terakhir, https://www.kompas.com/tren/read/2024/07/01/150000265/menkominfo-sebut-anggaran-bssn-terbatas-benarkah-ini-besarnya-5-tahun?page=all , diakses tanggal 12 Februari 2025

Dina Karina, Pusat Data Nasional Belanjakan Anggaran Rp 700 M sepanjang 2024, Tapi Kini Terkena Serangan Siber, https://www.kompas.tv/ekonomi/518371/pusat-data-nasional-belanjakan-anggaran-rp700-m-sepanjang-2024-tapi-kini-terkena-serangan-siber?page=all , diakses tanggal 27 Juni 2024

Ertugul A, 14 Mei 2023, Is SIEM Really Dead? Does XDR or Other Technologies Replace SIEM? What Types Of Attacks Does SIEM Detect?, https://www.linkedin.com/pulse/siem-really-dead-does-xdr-other-technologies-replace-what-akbas/ , diakses tangal 12 Oktober 2024

Hafidz Mubarak, 29 Juni 2024, Deret Layanan Terdampak Peretasan Pusat Data Nasional, https://www.cnnindonesia.com/nasional/20240628202216-12-1115511/deret-layanan-terdampak-peretasan-pusat-data-nasional , diakses tanggal 29 Juni 2024

Susy Ariyanie Yusuf, 5-6 Desember 2024, Aspek Legal dan Etika Penggunaan Data Pasien Dalam Teknologi *Big Data* dan Kecerdasan Buatan di Sektor Kesehatan, https://share.google/DDwTNjHNOlbQHmdk6 , diakses tanggal 26 September 2025

Teori Kedaulatan: Tuhan, Raja, Rakyat, Negara dan Hukum, 10 Februari 2023,
Hukum Online, 10 Februari 2023, 5 Teori Kedaulatan : Tuhan, Raja Rakyat, Negara, dan Hukum https://www.hukumonline.com/berita/a/teori-kedaulatan-lt62fa0ca6652f6/?page=all , diakses pada 15 April 2025

Mardhani Riasetiawan, 2020, Pusat Data Untuk Pemerintahan, https://cloud.wg.ugm.ac.id/wp-content/uploads/sites/1288/2020/11/Pusat-Data-untuk-Pemerintahan.pdf , diakses tanggal 08 Agustus 2024

Wahyu Sudoyo, 1 Juni 2022, Ini Langkah Indonesia Cegah Kebocoran Data, https://infopublik.id/kategori/nasional-sosial-budaya/636619/ini-langkah-indonesia-cegah-kebocoran-data , diakses tanggal 2 juli 2024