QISTINA: Jurnal Multidisiplin Indonesia
Vol. 3 No. 2 Desember 2024
P-ISSN: 2964-6278 E-ISSN: 2964-1268

Korelasi Hak & Kewajiban Warga Negara & Negara Dalam Perlindungan Data Pribadi (Menyoroti Kasus Peretasan Data Nasional)

Halimatun Sakdiah[1] Nadiyah[2] Geby Theresa Ginting[3] Mayland Gea[4] Neri Aisyah[5] Agtrimas Situmorang[6] Sanjaya Harahap[7] Taufiq Ramadhan[8]
Program Studi Pendidikan Fisika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan, Kota Medan, Provinsi Sumatera Utara, Indonesia[1,2,3,4,5,6,7,8]
Email: halimatunsakdiah@gmail.com[1] nadiyahyaya5@gmail.com[2] gebytheresia9@gmail.com[3] maylandgea7@gmail.com[4] neriaisyah14@gmail.com[5] agtrisitumorang37@gmail.com[6] sanjaya03sanjaya09@gmail.com[7] taufiqRamadhan@unimed.ac.id[8]

Abstrak

Penelitian ini menganalisis insiden peretasan yang terjadi pada Pusat Data Nasional (PDN) Indonesia pada 20 Juni 2024, yang mengakibatkan gangguan signifikan terhadap berbagai layanan pemerintah. Penelitian ini bertujuan untuk memahami karakteristik serangan siber, modus operandi ransomware jenis BrainChipper, dan kelemahan sistem keamanan yang menyebabkan kebocoran data. Dengan menggunakan pendekatan deskriptif dan analisis konten dari berbagai sumber, studi ini mengevaluasi dampak jangka pendek dan panjang dari peretasan tersebut, termasuk kerusakan operasional, penurunan kepercayaan publik, dan risiko terhadap keamanan nasional. Temuan menunjukkan pentingnya reformasi kebijakan keamanan siber dan penguatan infrastruktur teknologi informasi. Penelitian juga menyoroti tanggung jawab pemerintah dalam melindungi data pribadi dan memberikan penanganan yang efektif terhadap insiden kebocoran data untuk mencegah kejadian serupa di masa depan.
Kata Kunci: Peretas, Hukum, Data, Siber

Abstract

This study analyzed the incidence of hacking that occurred at the Indonesian National Data Center (PDN) on June 20, 2024, which resulted in a significant disruption to various government services. This study aims to understand the characteristics of cyber attacks, mode operandi ransomware type brainchipper, and the weakness of the security system that causes the leaking of data. By using a descriptive approach and content analysis of various sources, this study has a short and long-term impact of the hacking, including operational damage, a decrease in public trust, and risk to national security. The findings show the importance of reforming the Siber security policy and the strengthening of information technology infrastructure. The study also highlights the responsibility of the government in protecting personal data and providing effective handling of the incident of leaking data to prevent similar events in the future.
Keyword: *Hacking, Law, Data, Cyber*

PENDAHULUAN

Pusat Data Nasional (PDN) merupakan fasilitas pusat data untuk keperluan penempatan, penyimpanan dan pemrosesan data, serta pemulihan data yang nantinya digunakan untuk berbagi data secara terpusat instansi dan pemerintah daerah, serta saling berhubungan di Indonesia (Najwa, 2024). Pusat Data (Data Center) adalah suatu fasilitas gedung yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkait, misalnya seperti sistem telekomunikasi dan penyimpanan data. Pusat data besar fasilitas beroperasi pada skala industri menggunakan listrik sebanyak kota kecil (Fitrian, 2023). Pusat Data Nasional (PDN) merupakan pusat data (server) tempat data negara meliputi data dimiliki oleh Kementerian dan Lembaga. Pusat Data Nasional (PDN) merupakan

negara yang sangat penting pusat data yang keamanan dan kerahasiaannya harus dijaga setiap saat (Adristi & Ramadhani, 2024).

Di era digital yang semakin terhubung, keamanan data nasional menjadi salah satu prioritas utama bagi setiap negara. Pusat Data Nasional (PDN) merupakan tulang punggung berbagai layanan digital pemerintah, sehingga kebocoran data bisa berakibat serius berdampak pada keamanan nasional dan kepercayaan publik. Manajemen krisis dan respons insiden yang efektif adalah hal yang penting penting untuk meminimalkan dampak dari insiden ini. data nasional, sebagai tulang punggung infrastruktur digital suatu negara, menyimpan dan mengelola informasi kritis yang mencakup data pemerintahan, informasi pribadi warga negara, hingga rahasia negara yang sensitif. Namun, seiring dengan meningkatnya ketergantungan pada teknologi digital, ancaman siber terhadap aset-aset informasi ini juga semakin meningkat dalam hal kompleksitas dan frekuensi (Ramadhan et al., 2024).

Pada saat ini Pusat Data Nasional (PDN) menjadi perhatian masyarakat, tokoh IT dan DPR ketika Pusat Data Nasional diserang/diretas oleh peretas sehingga pusat data tidak dapat diakses. Serangan siber yang terjadi sejak Kamis (20/6/2024) melumpuhkan sejumlah layanan, termasuk layanan imigrasi. Tak hanya itu, penyerangan tersebut juga mengakibatkan hilangnya 282 data pemerintah instansi yang disimpan di PDN dikunci dan disandera hacker (Kompas.com, 26 Juni 2024). Insiden pembobolan Pusat Data Nasional (PDN) menyoroti kerentanan masyarakat Indonesia infrastruktur teknologi informasi pemerintah terhadap serangan cyber. Peristiwa ini bukan hanya menunjukkan kerentanan dalam sistem keamanan yang ada, tetapi juga mengungkapkan potensi dampak luas yang dapat ditimbulkan oleh serangan siber terhadap infrastruktur kritis nasional. Insiden ini telah memicu kekhawatiran serius di kalangan pembuat kebijakan, ahli keamanan, dan masyarakat umum tentang kesiapan negara dalam menghadapi ancaman siber yang semakin canggih. Peretasan tersebut telah mengakibatkan kebocoran data sensitif, gangguan layanan publik, dan berpotensi merusak kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi informasi penting. Lebih jauh lagi, insiden ini telah menimbulkan pertanyaanpertanyaan kritis tentang implikasi jangka panjang terhadap keamanan nasional, privasi individu, dan bahkan hubungan diplomatik internasional (Ma'ruf, 2024).

Berdasarkan latar belakang diatas, penelitian ini bertujuan untuk menganalisis secara mendalam insiden peretasan pusat data nasional yang terjadi pada Kamis (20/6/2024), dengan fokus pada karakteristik dan modus serangan serta kelemahan sistem keamanan yang teridentifikasi. Studi ini akan menyelidiki implikasi jangka pendek dan jangka panjang dari peretasan tersebut, meliputi dampaknya terhadap keamanan informasi negara, kepercayaan publik dalam pengelolaan data pemerintah, Penelitian akan mengkaji efektivitas tindakan perlindungan data yang telah diterapkan sebelum terjadinya insiden dan mengidentifikasi langkah-langkah perbaikan serta peningkatan keamanan yang diperlukan untuk mencegah peretasan serupa di masa depan. Dalam konteks ini, akan dieksplorasi strategi komprehensif untuk meningkatkan ketahanan siber nasional, khususnya dalam melindungi pusat data strategis. Penelitian ini akan mendalami peran dan tanggung jawab pemerintah serta Menteri Komunikasi dan Informatika (Menkominfo) dalam penguatan perlindungan data nasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dengan metode analisis konten. Pendekatan ini dipilih untuk memungkinkan pemahaman mendalam tentang peretasan pusat data nasional, implikasinya, dan tindakan perlindungan data yang relevan. Data akan dikumpulkan dari berbagai artikel ilmiah, laporan teknis, berita, dan dokumen kebijakan yang berkaitan dengan peretasan pusat data, keamanan siber nasional, dan perlindungan data.

Sumber-sumber ini akan mencakup jurnal ilmiah di bidang keamanan informasi dan cyber security dan artikel berita dari sumber-sumber terpercaya yang melaporkan insiden peretasan. Penelitian ini terbatas pada analisis dokumen dan tidak melibatkan pengumpulan data primer atau wawancara dengan pihak-pihak yang terlibat dalam insiden peretasan atau manajemen keamanan data nasional.

HASIL PENELITIAN DAN PEMBAHASAN

Implikasi Kasus Peretasan Pusat Data Nasional Bagi Warga Negara

Pada tanggal 17 Juni 2024 pukul 23.15 WIB, peretas berhasil menonaktifkan fitur keamanan Windows Defender di PDNS 2 di Surabaya. Hal ini memungkinkan aktivitas berbahaya untuk beroperasi. Tiga hari kemudian, pada tanggal 20 Juni 2024 pukul 00.54 WIB, aktivitas berbahaya seperti instalasi file berbahaya, penghapusan file system penting, dan penonaktifan layanan berjalan mulai terjadi. Pada pukul 00.55 WIB, Windows Defender mengalami crash dan tidak dapat beroperasi, sehingga sistem menjadi rentan terhadap serangan ransomware. Peretas menggunakan ransomware bernama Brain Cipher Ransomware, yang merupakan pengembangan terbaru dari ransomware LockBit 3.0. Mereka meminta tebusan sebesar USD 8 juta (sekitar Rp131 miliar). Serangan ini menyebabkan gangguan pada sejumlah layanan publik, termasuk imigrasi. Sebanyak 282 instansi terdampak, dan 239 di antaranya mengalami gangguan layanan mereka.Tim dari Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), Polri, dan Telkom melakukan upaya untuk memulihkan data yang tersandera. Namun, upaya ini tidak berhasil melawan serangan ransomware. Kronologi serangan ini dijelaskan oleh Menteri Komunikasi dan Informatika Budi Arie Setiadi dalam rapat kerja dengan Komisi I DPR RI. Serangan dimulai dari pembobolan Windows Defender hingga instalasi file berbahaya dan penonaktifan layanan berjalan. kompas.com, 24 Juni 2024.

Indonesia menghadapi krisis serius terkait pencurian identitas yang mempengaruhi jutaan warganya. Kasus penipuan yang melibatkan KTP palsu dan penyalahgunaan Nomor Induk Kependudukan (NIK) meningkat tajam setelah peretasan data, menyebabkan kerugian finansial yang signifikan. Banyak korban melaporkan adanya transaksi mencurigakan di rekening bank mereka; beberapa mengalami pencurian uang secara langsung, sementara yang lain menjadi sasaran penipuan online yang canggih. Ancaman terhadap privasi semakin nyata, dengan informasi pribadi seperti riwayat medis, status perkawinan, dan detail keluarga bocor ke publik, menciptakan rasa tidak aman di kalangan masyarakat. Selain itu, beredar kabar bahwa data yang dicuri digunakan untuk kepentingan politik, seperti manipulasi pemilih menjelang pemilu, serta untuk pemasaran agresif oleh perusahaan yang tidak bertanggung jawab. Kepercayaan publik terhadap kemampuan pemerintah dalam menjaga keamanan data anjlok drastis, memicu demonstrasi dan protes di berbagai kota besar. Lebih parah lagi, bocornya dokumen pemerintah rahasia menimbulkan kekhawatiran akan keamanan nasional, dengan spekulasi bahwa negara asing mungkin telah mendapatkan akses ke informasi strategis Indonesia (Sadikin et al., 2024).

Negara Menjamin Hak Perlindungan Data Pribadi Warga Negara

1. Jaminan melalui Pasal 28G ayat (1) UUD 1945 Pasca insiden, pemerintah Indonesia menegaskan kembali komitmennya terhadap Pasal 28G ayat (1) UUD 1945. Pasal ini, yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, menjadi landasan utama dalam upaya pemulihan kepercayaan publik. Pemerintah menggunakan pasal ini sebagai dasar untuk memperkuat regulasi dan sistem perlindungan data.

2. Penerapan UU Perlindungan Data Pribadi (UU 27/2022) Pengaturan tentang perlindungan data pribadi, pemerintah mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang memberikan perlindungan terhadap data-data dalam server PDN. Pasal 1 ayat (2) UU PDP menyatakan bahwa perlindungan data pribadi adalah sebuah upaya untuk melindungi data hingga menjamin pemrosesan data pribadi seseorang dengan aman. Proses perlindungan data pribadi tersebut akan dilakukan oleh pengendali data pribadi yang dalam Pasal 1 ayat (4) UU PDP disebutkan salah satunya adalah pemerintah. Dengan begitu, server PDN yang berisikan data-data pribadi milik masyarakat sudah seharusnya dijaga dan dilindungi sebaik mungkin oleh pemerintah.
3. Penguatan UU ITE Peretasan terhadap server PDN tentu dapat dijerat menggunakan regulasi hukum. Berdasarkan Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), tindakan yang dilakukan sengaja maupun tidak sengaja dengan menerobos hingga menjebol sistem pengaman suatu sistem elektronik merupakan perbuatan yang dilarang. Melalui Pasal 46 ayat (3) dan Pasal 52 ayat (3) UU ITE mengatur terkait ancaman pidana penjara terhadap pelaku peretasan sistem pemerintah selama 8 tahun ditambah dua pertiga. Namun, regulasi hukum yang ada ini belum cukup kuat untuk mencegah adanya tindakan peretasan dan kebocoran data pribadi. Diperlukan regulasi yang tidak hanya mengatur mengenai tindakan yang dilarang, tetapi juga mengatur keamanan dan perlindungan terhadap data-data yang ada di dalam nya (Najwa, 2024).
4. Langkah yang dapat dilakukan pemerintah atas insiden ini Untuk mengatasi insiden ini, terdapat beberapa tindakan yang dapat ditingkatkan atau diperbaiki oleh pemerintah. Pertama adalah mengenai segi regulasi yang berlaku. Saat ini ketentuan yang ada masih belum berupa undang-undang khusus mengenai keamanan siber. Undang-undang diperlukan untuk menjadi standar dalam penanganan secara sigap jika terjadi insiden serupa. Pasca insiden PDN, Badan Siber Sandi Negara (BSSN) menyoroti bahwa salah satu rentannya Indonesia terhadap ancaman siber karena ketiadaan UndangUndang Keamanan Siber. Saat ini pemerintah perlu segera mengesahkan RUU Keamanan Siber untuk dapat menjadi standar yang secara komprehensif dan spesifik mengatur tata kelola keamanan siber di Indonesia, serta meningkatkan kepercayaan masyarakat.

Mengenai segi sistem keamanan. Seharusnya terdapat standar sistem keamanan untuk institusi pemerintah, seperti PDN, yang telah teruji. Sistem keamanan tersebut juga harus di-upgrade dan ditingkatkan secara berkala untuk menghindari ketertinggalan sistem. Diperlukan juga untuk melakukan cyber security testing, terdiri dari cybersecurity audit, penetration test, vulnerability scan, security scan, risk assessment, dan posture assessment yang secara keseluruhan merupakan rangkaian tes uji coba untuk melihat tingkat keamanan dari sistem yang digunakan. Langkah lainnya adalah dengan meningkatkan kemampuan sumber daya manusia yang ada. Pemerintah perlu melakukan pelatihan dan pendidikan secara berkala kepada ahli teknisi agar lebih siap dalam menghadapi serangan siber yang dilakukan para peretas. Para ahli teknisi yang ada juga perlu melakukan uji coba atau praktik secara berkala dan pemahaman pola pikir para peretas agar siap beberapa langkah ke depan sebelum insiden terulang. Melalui tata kelola dan persiapan matang, Indonesia diharapkan dapat mengikuti perkembangan zaman yang begitu pesat dalam bidang teknologi dengan lebih baik. Pemerintah Indonesia haruslah siap untuk menghadapi insiden serupa di kemudian hari melalui evaluasi yang lebih baik (Fitrian, 2023). Dalam kasus peretasan Pusat Data Nasional (PDN), terdapat beberapa pasal hukum yang dapat diterapkan, baik dari Kitab Undang-Undang Hukum Pidana (KUHP) maupun Undang-Undang Informasi dan Transaksi

Elektronik (UU ITE). Berikut adalah penjabaran lebih lengkap dan akurat mengenai pasal-pasal yang relevan:

1. Pasal 30 UU ITE (No. 11 Tahun 2008 sebagaimana telah diubah dengan UU No. 19 Tahun 2016 dan Perubahan Kedua dengan UU No. 1 Tahun 2024): Pasal ini mengatur tentang larangan setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Sistem elektronik milik orang lain dengan cara apa pun. Pelanggaran terhadap pasal ini dapat dikenakan sanksi pidana berupa pidana penjara paling lama 8 (delapan) tahun.
2. Pasal 32 UU ITE Pasal ini mengatur tentang larangan setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen elektronik milik orang lain atau milik publik. Pelanggaran terhadap pasal ini dapat dikenakan sanksi pidana berupa pidana penjara paling lama 8 (delapan) tahun.
3. Pasal 46 UU ITE Pasal ini mengatur tentang sanksi pidana bagi pelanggaran yang dilakukan terhadap ketentuan dalam UU ITE, termasuk tindakan peretasan yang mengakibatkan kerugian bagi orang lain. Sanksi pidana yang dapat dikenakan berupa pidana penjara paling lama 10 (sepuluh) tahun.
4. Pasal 362 KUHP (Pencurian) Pasal ini mengatur tentang tindak pidana pencurian, yang dapat diterapkan jika data yang dicuri dalam peretasan dianggap sebagai barang yang dapat dicuri. Sanksi pidana yang dapat dikenakan berupa pidana penjara paling lama 5 (lima) tahun.

Korelasi Hak & Kewajiban Warga Negara & Negara Dalam Perlindungan Data Pribadi

Kasus kebocoran data yang meluas ini telah menjadi studi kasus utama dalam kurikulum Pendidikan Kewarganegaraan di sekolah-sekolah Indonesia, menggambarkan perlunya keseimbangan antara hak privasi individu dan kebutuhan akan keamanan nasional. Pemerintah Indonesia mengakui kegagalannya dalam melindungi data pribadi warga dan merespons dengan berbagai langkah. Pertama, mereka menyediakan kompensasi finansial bagi korban yang mengalami kerugian langsung akibat kebocoran data. Selain itu, pemerintah membentuk tim khusus untuk membantu korban memulihkan identitas digital mereka dan melakukan restrukturisasi menyeluruh terhadap sistem keamanan data nasional. Insiden ini menyebabkan masyarakat menjadi lebih sadar akan hak-hak mereka terkait data pribadi, dengan permintaan akses dan koreksi data pribadi ke lembaga pemerintah meningkat signifikan. Gerakan "Right to be Forgotten" mendapatkan popularitas, dengan banyak warga yang meminta penghapusan data mereka dari sistem pemerintah yang dianggap tidak esensial. Korelasi antara insiden ini dan perubahan dalam hubungan negara dengan warga negara menciptakan paradigma baru dalam pengelolaan data pribadi. Warga negara menjadi lebih proaktif dalam menjaga keamanan data mereka, sementara pemerintah menjadi lebih transparan dalam pengelolaan data. Forum-forum diskusi reguler antara pemerintah dan masyarakat sipil mengenai kebijakan data dibentuk, dan konsep "data sebagai aset nasional" mulai diterima secara luas. Konsep ini menggarisbawahi bahwa perlindungan data adalah tanggung jawab bersama. Undang-undang baru memperkenalkan konsep "hak veto data," yang memberikan hak kepada warga untuk menolak penggunaan data mereka untuk tujuan tertentu oleh pemerintah. Peristiwa peretasan 2024 ini menjadi titik balik dalam sejarah perlindungan data di Indonesia. Meskipun awalnya merupakan tragedi nasional, insiden tersebut akhirnya mendorong perkembangan signifikan dalam hal kebijakan, teknologi, dan kesadaran masyarakat tentang pentingnya keamanan data pribadi.

KESIMPULAN

Serangan siber terhadap Pusat Data Nasional (PDN) pada tanggal 20 Juni 2024 merupakan insiden yang signifikan dalam sejarah keamanan siber Indonesia. Serangan ini dilakukan menggunakan ransomware BrainChipper yang menginfeksi server PDN di Surabaya dan mengenkripsi data di dalamnya. Serangan ini menyebabkan gangguan pada layanan publik di 210 instansi pemerintah, termasuk layanan imigrasi dan aplikasi penting seperti SINDE dan KIP-Kuliah. Serangan ini juga mengakibatkan hilangnya 282 data pemerintah yang disimpan di PDN, dengan hacker meminta tebusan sebesar US$ 8 juta. Pemerintah bersikap tegas dan tidak akan membayar uang tebusan tersebut. Upaya pemulihan sedang dilakukan secara bertahap untuk mengembalikan fungsi layanan publik yang terdampak. Pemerintah juga berencana untuk memperkuat sistem keamanan siber nasional agar kejadian serupa tidak terulang kembali di masa mendatang. Peretasan ini menyoroti kerentanan infrastruktur teknologi informasi pemerintah terhadap serangan cyber dan mengungkapkan potensi dampak luas yang dapat ditimbulkan oleh serangan siber terhadap infrastruktur kritis nasional. Insiden ini telah memicu kekhawatiran serius di kalangan pembuat kebijakan, ahli keamanan, dan masyarakat umum tentang kesiapan negara dalam menghadapi ancaman siber yang semakin canggih. Peretasan ini juga menegaskan pentingnya manajemen krisis dan respons insiden yang efektif untuk meminimalkan dampak dari insiden ini.

DAFTAR PUSTAKA

Adristi, F. I., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. Jurnal Mahasiswa Bisnis & Manajemen, 02(06), 196–212.

Fitrian, Y. (2023). Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara. Arus Jurnal Sosial Dan Humaniora, 3(3), 164–174.

Ma'ruf, S. (2024). Manajemen Krisis dan Respons Insiden: Studi Kasus Pusat Data Nasional. Journal Intelek Dan Cendikiawan Nusantara, 1(3), 4619–4633.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. Jurnal Ilmu Sosial, Politik, Dan Hukum, 2(1), 8–16.

Ramadhan, T. wahyu, Florina, I. D., & Permadi, D. (2024). Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo.co. Journal of Education Research, 5(3), 3368–3379.

Sadikin, J., Azis, A., & Putra, M. (2024). Melacak Tantangan Peretasan dalam Perkembanga Dunia Maya di Indonesia. Jurnal Hukum Agama Hindu, 14(1), 24–39.