(2023), 1 (2): 65–72 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

MENJAGA HAK DIGITAL WARGA NEGARA DI ERA TERBUKA: MENGEMBANGKAN STANDAR PERLINDUNGAN DATA YANG DEMOKRATIS DALAM LAYANAN BPJS

Adhisya Naira Fayyaza, Rahima Putri Anggita Sipayung, Vanessa Maheswari Nugroho
Departemen Ilmu Administrasi Negara, Fakultas Ilmu Administrasi, Universitas Indonesia
adhisya.naira@ui.ac.id , rahima.putri@ui.ac.id , vanessa.maheswari@ui.ac.id

Abstrak

Perkembangan industri yang memasuki tahap 4.0 dimana industri teknologi dunia semakin berkembang membuat peningkatan penggunaan teknologi informasi menjadi ujung tombak dalam pelaksanaan seluruh administrasi organisasi menjadi sangat pesat dan membuat sebuah peluang besar dalam menciptakan ancaman baru bagi keberlangsungan demokrasi terutama di Indonesia.. Ancaman tersebut dapat berupa kebocoran data siber yang dianggap sebagai suatu masalah yang serius. Perlindungan data menjadi sebuah aspek kritis untuk menjamin setiap hak-hak digital individu yang bersifat privasi di dalamnya. Sehingga, tantangan terhadap keamanan data siber menjadi hal yang harus ditingkatkan terutama dalam menjaga keamanan privasi setiap individu dalam setiap institusi maupun lembaga publik. Artikel ini membahas lebih dalam mengenai keterkaitan antara keamanan siber, perlindungan data pribadi, dan kaitannya dengan demokrasi di dalamnya. Demokrasi seringkali dihubungkan dengan perlindungan Hak Asasi Manusia, dalam keamanan data siber dimana memainkan peran dalam melindungi setiap privasi individu, tentu harus dijaga dari potensi penyalahgunaan data oleh pihak yang tidak berwenang. Kebocoran data yang mengungkap informasi pribadi masyarakat tentu dinilai sebagai sebuah pelanggaran privasi dan Hak Asasi Manusia yang seharusnya dilindungi untuk memastikan partisipasi bebas dan adil dalam setiap proses demokratis. Kebocoran data pribadi adalah pelanggaran etika karena merugikan hak individu untuk menjaga privasinya, sehingga etika memainkan peran sentral dalam memandu tindakan yang membentuk kebijakan dan praktik terkait keamanan data dalam upaya menjaga integritas demokrasi.

Kata Kunci : Keamanan Data, Demokrasi, Perlindungan Data Pribadi

PENDAHULUAN

Dengan perkembangan teknologi informasi dan komunikasi (TIK) beberapa dekade terakhir yang kian pesat, penggunaan internet dan *big data* tidak dapat dipisahkan dari berbagai sendi kehidupan manusia.Teknologi digital menjadi sebuah kunci dalam kemudahan akses internet dan semua aspek kehidupan menjadi lebih efisien dan fleksibel. Dengan dorongan kemajuan teknologi informasi, hak digital warga negara menjadi sebuah aspek krusial dalam mendukung prinsip-prinsip demokrasi dan mencerdaskan kehidupan bangsa. Perkembangan pesat akan teknologi informasi tersebut tentu membawa pengaruh dan manfaat besar bagi keberlangsungan kehidupan seperti mudahnya mengakses berbagai informasi yang ada dalam lingkup publik. Penggunaan dan ketergantungannya terhadap teknologi selain pada individu, Institusi dan lembaga pemerintahan di Indonesia pun ikut serta dalam pemanfaatan TIK guna memberikan layanan yang lebih baik dan efisien bagi masyarakat, sehingga keamanan dalam data siber menjadi hal yang relevan dan sangat penting. Salah satu institusi yang memanfaatkan *database* dan digitalisasi pelayanan di Indonesia adalah BPJS (Badan Penyelenggara Jaminan Sosial). Terdapat lebih dari 200 juta jiwa data yang telah dicatat dan dikelola oleh BPJS baik itu data kesehatan maupun data ketenagakerjaan seperti jaminan sosial di Indonesia. Data yang dikelola pun sangat beragam, mulai dari identitas diri yang dinilai sensitif seperti NIK, nomor KK dan KTP, alamat rumah, sidik jari pengesahan, hingga detail medis lainnya.

Namun, disisi lain, perkembangan tersebut menghadirkan tantangan serius terkait dengan keamanan dan privasi data dari setiap individu yang menggunakkan teknologi informasi. Kebocoran data pribadi misalnya, memiliki potensi yang signifikan untuk mempengaruhi demokrasi suatu negara karena mengancam privasi warga negara. Dengan informasi pribadi yang tersebar secara tidak sah, dapat merusak kepercayaan masyarakat terhadap integritas institusi terikat yang dapat mempengaruhi bagaimana warga negara turut

berpartisipasi dalam pelaksanaan maupun pelayanan publik yang disediakan oleh negara. Sehingga, hak digital, mencakup keamanan data dan privasi dari setiap individu menjadi tanggungjawab negara dalam memastikan keamanan dan kesejahteraan setiap individu warga negara didalamnya. Kekhawatiran terhadap serangan data siber tersebut tentu mendorong pemerintah dan penyelenggara sistem elektronik (PSE) untuk meningkatkan perlindungan sistem dan penanganan terhadap serangan siber.

Konsep Demokrasi dan kaitannya dengan TIK

Demokrasi memiliki kaitan erat dengan kebebasan, yang pada dasarnya merupakan suatu sistem politik dimana rakyat atau warga negara memiliki kedaulatan untuk menentukan pemimpin dan kebijakan-kebijakan yang akan ditetapkan, baik secara langsung maupun melalui para wakil rakyat. Demokrasi juga menjunjung nilai-nilai kebebasan dalam berekspresi, kesetaraan, serta partisipasi warga negara. Dahl (1996) menekankan demokrasi deliberatif, di mana diskursus publik yang rasional sangat penting untuk pengambilan keputusan demokratis. Demokrasi dipercaya sebagai bentuk pemerintahan terbaik karena minimnya potensi tirani dan adanya mekanisme *checks and balances* serta pemilihan berkala. Secara umum, demokrasi bertujuan untuk mencapai aspirasi rakyat dan melindungi kepentingan publik. Demokrasi dipandang sebagai bentuk pemerintahan terbaik karena partisipasi luas dan perwakilan politik yang akuntabel.

Demokrasi juga didefinisikan sebagai sistem nilai, sikap, dan praktik dalam sebuah pemerintahan yang mengedepankan partisipasi rakyat. Nilai-nilai demokrasi tersebut bisa diimplementasikan dengan cara yang berbeda-beda pada setiap negara dan budaya. Meski begitu, ada prinsip-prinsip umum penyelenggaraan negara demokratis yang bisa dijadikan standar evaluasi bagi setiap demokrasi modern di dunia. Prinsip-prinsip tersebut meliputi partisipasi warga negara dalam proses politik, kesetaraan di depan hukum, toleransi politik atas perbedaan, transparansi dan akuntabilitas pemerintahan, adanya pemilu berkala yang bebas dan adil, kebebasan ekonomi yang diatur regulasi, kontrol terhadap penyalahgunaan kekuasaan, perlindungan HAM, sistem multi partai, netralitas institusi negara dan tegaknya rule of law. Dengan prinsip-prinsip demokrasi yang dijaga dengan konsisten, sebuah negara dapat terus melanjutkan konsolidasi demokrasi dan legitimasi sistem pemerintahan yang ada di mata rakyat.

Terdapat kaitan yang erat antara demokrasi dan perkembangan teknologi informasi dan komunikasi. Perkembangan yang kian pesat dari teknologi informasi dan komunikasi juga ikut terlibat dalam mempengaruhi demokrasi dan sistem politik negara secara signifikan. TIK seperti media sosial, platform digital, dan internet membantu demokratisasi informasi serta partisipasi masyarakat luas. Melalui platform digital, warga negara dapat secara mudah untuk mengakses segala informasi yang disediakan oleh pemerintah sehingga dapat memperbaiki transparansi, akuntabilitas, dan kepercayaan publik terhadap pemerintah. Di sisi lain, perkembangan TIK dan penggunaan *e-government* berpotensi membawa risiko seperti kebocoran data, penyebaran hoaks, dan kejahatan siber lainnya yang dapat mengancam proses dan nilai-nilai demokrasi.

METODE PENELITIAN

Metode penelitian yang digunakkan dalam penulisan artikel ini didasarkan pada analisis literatur yang melibatkan kajian mendalam terhadap sumber sumber bacaaan yang relevan. Langkah awal dalam penulisan artikel ini melibatkan identifikasi sumber-sumber utama yang menyediakan teori konseptual yang berhubungan dengan toik. Sumber-sumber bacaan yang diambil dalam artikel ini meliputi jurnal ilmiah, buku, maupun artikel yang membahas isu mengenai kebocoran data pribadi, penyebab kebocoran data pribadi, dan

bagaimana dampak dan pengaruhnya terhadap demokrasi serta stabilitas negara. Analisis literatur ini juga melibatkan pembacaan kritis terhadap berbagai teori dan temuan penelitian yang ditemukan dalam proses penulisan artikel ini guna membangun kerangka analisis yang mendalam dan kuat. Dengan pendekatan analisis dalam artikel ini, diharapkan dapat memberikan kontribusi pada pemahaman yang lebih dalam mengenai kompleksitas isu kebocoran data pribadi yang telah terjadi dan relevansinya dengan demokrasi dan stabilitas negara.

HASIL PENELITIAN DAN PEMBAHASAN

a. Definisi keamanan siber dan pentingnya keamanan siber dalam era digital dalam institusi publik

Penggunaan internet yang semakin luas telah meningkatkan peningkatan serangan siber. Dalam era di mana institusi publik semakin bergantung pada teknologi informasi untuk mengelola dan melakukan aktivitas publik, maka keamanan siber menjadi hal yang paling fundamental untuk memitigasi risiko terhadap ancaman siber yang tentu dapat merugikan kepercayaan publik itu sendiri. Keamanan siber menjadi hal yang sangat krusial dalam pelaksanaan setiap aktivitas pelayanan publik bagi institusi publik yang menyangkut berbagai data pribadi milik masyarakat. Keamanan siber merupakan sebuah upaya perlindungan dan pengamanan perangkat dari adanya ancaman maupun serangan oleh pihak yang tidak bertanggung jawab. Keamanan siber adalah praktek untuk menjaga sistem komputer, jaringan, dan data agar terhindar dari pencurian, kerusakan, atau akses yang tidak sah. Signifikansinya semakin meningkat di era digital, terutama bagi entitas publik yang menyimpan informasi sensitif dan bertanggung jawab atas infrastruktur serta layanan krusial. Keamanan siber memainkan peranan penting terutama dalam perlindungan data pribadi termasuk informasi, identitas, informasi keuangan, dan informasi penting lainnya dalam institusi publik. Institusi publik tentu mengelola dan menyimpan banyak data sensitif. Hal ini berhubungan dengan kepercayaan masyarakat terkait keberhasilan serta integritas yang dimiliki oleh institusi publik dalam menjaga privasi data-data pribadi yang diberikan oleh masyarakat. Maka dari itu, keamanan siber yang kuat dapat membantu institusi publik mempertahankan kepercayaan masyarakat dengan menunjukkan komitmen mereka dalam melindungi informasi pribadi. Terlebih lagi di zaman sekarang, institusi publik semakin bergantung pada teknologi dan layanan digital, perlindungan keamanan siber menjadi semakin krusial untuk mendukung proses transformasi digital dan memastikan keberhasilannya.

Oleh karena itu, penting untuk menciptakan kebijakan dan pengimplementasian praktik keamanan siber yang canggih dan adaptif menjadi imperatif untuk menjaga keandalan, kepercayaan dari institusi publik terkait dalam menghadapi tantangan maupun ancaman yang terus berkembang di ranah siber.

b. Keterkaitan antara keamanan siber dan perlindungan data dalam demokrasi

Semakin meningkatnya tantangan yang dihadapi oleh negara-negara demokratis dalam mengelola aspek kompleks keamanan siber telah menjadi perhatian utama dalam kebijakan domestik dan luar negeri, yang memiliki dampak langsung pada hak asasi manusia dan stabilitas demokrasi suatu negara.

Keamanan siber adalah isu multidimensi yang melibatkan aspek hukum, diplomasi, teknologi IT, pertahanan, keselamatan masyarakat, ekonomi, serta HAM. Dalam setiap data siber yang didalamnya terdapat hak hak individu dan data pribadi memiliki dampak yang sangat relevan terhadap keseimbangan demokrasi yang dimana inti dari prinsip demokrasi adalah menjamin kesejahteraan dan perlindungan individu termasuk hak dan privasi yang tertuang dalam data-data pribadi dalam lingkungan digital di dalam demokrasi modern ini.

Keamanan siber dan perlindungan data memiliki peranan yang sangat krusial dalam memelihara prinsip demokrasi di zaman digital saat ini. Dalam konteks demokrasi, keamanan siber bertindak sebagai penjaga yang melindungi integritas setiap institusi publik yang didalamnya terdapat data-data pribadi masyarakat. Sehingga, ketika data pribadi warga disimpan dan dikelola oleh institusi demokratis, perlindungan data menjadi hal yang paling esensial dalam mencegah potensi penyalahgunaan hingga peretasan oleh pihak yang tidak bertanggungjawab. Dalam konteks demokrasi juga, negara tentunya harus menjamin kesejahteraan dan keamanan yang tertuang dalam memastikan adanya perlindungan atas hak pribadi maupun individu yang tentunya juga berkaitan dengan keadilan sosial. Keamanan siber tidak hanya terdiri dari berbagai ancaman teknis, melainkan juga merupakan sebuah komponen keamanan manusia pada era digital saat ini. Kekurangan atau kualitas rendah dari keamanan siber dapat mengancam ruang demokrasi serta prinsip demokrasi itu sendiri. Oleh karena itu, strategi keamanan siber nasional perlu dibangun dengan pendekatan yang menyeluruh dan kolaboratif dari berbagai pemangku kepentingan. Melindungi infrastruktur digital yang sangat vital dan rawan diserang tersebut adalah keniscayaan bagi setiap negara demi menjaga keamanan nasional yang komprehensif, sesuai dengan konsep keamanan manusia di era globalisasi saat ini.

c. Ancaman dan risiko keamanan siber

Masifnya perkembangan teknologi menjadi salah satu alasan utama yang menyebabkan banyak aspek kehidupan manusia bergantung pada jaringan internet dan infrastruktur digital. Akibatnya, ancaman keamanan siber kini menjadi risiko yang sangat serius bagi kestabilan politik maupun kepercayaan warga negara terhadap pemerintah di era globalisasi. Maraknya serangan siber yang menyasar berbagai sistem seperti instansi publik, perbankan, transportasi, hingga pertahanan nasional dapat menimbulkan bencana dan kerugian yang sangat besar.

Ancaman keamanan siber adalah tindakan yang dilakukan untuk mengganggu, merusak, atau mengambil alih sistem komputer atau jaringan. Ancaman keamanan siber mengacu pada potensi risiko dan kerugian yang diakibatkan oleh serangan siber atau pelanggaran data pada suatu organisasi.

Ancaman keamanan siber dapat berasal dari berbagai sumber, termasuk individu, kelompok, atau negara. Beberapa ancaman utama terkait keamanan siber yang sedang marak terjadi seperti:

1. **Serangan Siber**

   Ancaman ini mencakup exploitasi celah keamanan sistem jaringan dengan melakukan peretasan dan penyusupan malware. Tujuannya bisa mencuri, mengubah, atau merusak data sensitif, mengganggu layanan penting bagi masyarakat, hingga memata-matai aktivitas korban. Beberapa jenis serangan siber yang umum ditemukan antara lain virus & *worm* (*malware* yang mereplikasi diri), *ransomware* (menyandera data penting dengan enkripsi), *distributed denial of service/DDoS* (membanjiri server dengan *request* berlebihan hingga *overload* & tak bisa melayani), *SQL injection* (menyisipkan kode berbahaya ke *database* melalui celah input), serta *phishing* (menipu korban untuk menyerahkan data sensitif).

2. **Pencurian Data**

   Risiko ini terkait hilang atau bocornya data-data sensitif akibat serangan atau kelalaian manusia. Data yang dicuri bisa beragam mulai dari informasi pribadi warga negara (KTP, nomor kartu kredit, alamat, dsb), data rahasia negara (dokumen pertahanan & diplomasi), hingga kekayaan intelektual perusahaan seperti rumus rahasia atau desain

produk. Akibatnya bisa sangat merugikan baik individu, pemerintah, maupun organisasi terkait.

3. **Kejahatan Siber Transnasional**
   Ancaman lain adalah makin canggih dan masifnya kejahatan siber transnasional terorganisir seperti penjualan data pribadi, narkoba, senjata, atau perdagangan manusia ilegal menggunakan dark web, mata uang kripto dan anonimitas dunia maya. Selain itu maraknya kasus penipuan daring yang merugikan masyarakat. Diperlukan kerja sama global dan kecanggihan teknis untuk menindak kejahatan internasional ini.

Sedangkan risiko keamanan siber adalah dampak yang mungkin terjadi dari serangan keamanan siber. Risiko keamanan siber dapat berupa kerugian finansial, kerusakan reputasi, atau gangguan operasional. Contohnya seperti:

1. **Kerugian finansial**
   Serangan keamanan siber dapat menyebabkan kerugian finansial bagi organisasi atau individu. Kerugian finansial dapat disebabkan oleh berbagai faktor, seperti biaya untuk memulihkan sistem yang rusak, biaya untuk membayar denda, atau biaya untuk mengganti data yang hilang.
2. **Kerusakan reputasi**
   Serangan keamanan siber dapat merusak reputasi organisasi atau individu. Kerusakan reputasi dapat menyebabkan hilangnya kepercayaan konsumen atau pelanggan, serta hilangnya bisnis.
3. **Gangguan operasional**
   Serangan keamanan siber dapat mengganggu operasional organisasi atau individu. Gangguan operasional dapat menyebabkan hilangnya produktivitas, hilangnya pendapatan, atau bahkan hilangnya nyawa.

d. Tinjauan studi kasus pelanggaran data yang mempengaruhi aspek demokrasi

Kasus kebocoran data pribadi telah menjadi sebuah hal yang semakin menunjukkan urgensi untuk ditetapkannya peraturan perundang-undangan perlindungan data pribadi karena hal ini menjadi hal yang sangat krusial. Salah satu kasus kebocoran data pribadi terjadi pada institusi lembaga publik yang bertanggung jawab dalam menyelenggarakan jaminan kesehatan nasional bagi seluruh rakyat indonesia, yaitu Badan Penyelenggara Jaminan Sosial Kesehatan atau yang lebih dikenal dengan BPJS Kesehatan. BPJS Kesehatan merupakan program pemerintah dalam kesatuan Jaminan Kesehatan Nasional yang juga menjalankan fungsi pemerintahan di bidang pelayanan umum (*public services)* di bidang penyelenggaraan jaminan sosial nasional kepada seluruh rakyat Indonesia. Sehingga, BPJS Kesehatan dalam pelaksanaan tugasnya, dipertanggungjawabkan kepada Presiden sebagai kepala pemerintahan negara.

Dalam proses pelaksanaan pelayanan publiknya, tentu BPJS Kesehatan menggunakan data pribadi setiap penggunanya sebagai syarat pelayanan BPJS Kesehatan. Namun, sekitar 279 Juta data warga Indonesia yang menggunakkan BPJS Kesehatan sebagai jaminan kesehatannya diduga diretas dan dijual dalam forum daring dari berbagai database yang terungkap pada bulan Mei 2021. Dalam hal ini, data berupa Nomor Induk Kependudukan (NIK), nama, alamat, e-mail, dan nomor telepon. Bocornya data BPJS Kesehatan ini tentu menimbulkan masyarakat tidak memiliki rasa aman dalam memberikan data-data pribadinya kepada instansi pemerintah maupun

pihak swasta sekalipun karena rentan menjadi korban kejahatan *cybercrime* ini. Peretasan situs web BPJS yang dilakukan oleh pihak tidak bertanggung jawab tersebut, secara tidak langsung menunjukkan masih lemahnya sistem keamanan yang dimiliki oleh BPJS Kesehatan. Disisi lain, tindakan peretasan dan penjualan data pribadi kepada berbagai database merupakan sebuah hal yang sangat tidak etis dan melanggar Hak Asasi Manusia atas penggunaan teknologi. Kebocoran data pribadi tentu akan memberikan dampak yang sangat serius terhadap banyak orang yang data pribadinya tersebar luas, karena hal ini berkaitan dengan privasi individu yang menjadi sasaran oleh pihak-pihak yang tidak bertanggung jawab. Hubungan antara tindak peretasan dengan etika menjadi hal yang sangat kompleks karena juga berhubungan dengan pelanggaran privasi dan integritas yang merugikan individu atau organisasi yang menjadi sasaran.

Kebocoran data pribadi juga tentunya dapat memberikan dampak potensial yang sangat meresahkan terhadap keseimbangan demokrasi hingga stabilitas negara. Kurangnya keamanan dalam penyimpanan data pribadi tentu memberikan peluang bagi para aktor yang tidak berwenang untuk dapat dengan mudahnya memanfaatkan informasi pribadi dalam praktik kejahatan seperti pencurian identitas hingga pemerasan yang tentunya membahayakan ketertiban sosial dan keamanan negara secara menyeluruh.

Ketika data pribadi bocor di dalam lembaga pemerintahan, hal ini dapat menimbulkan kekhawatiran masyarakat terhadap keamanan informasi pribadi mereka. Data yang diretas dapat mencakup rincian informasi pribadi. Terdapat keprihatinan bahwa data yang terbocor mungkin dimanfaatkan untuk kegiatan penipuan, seperti pengajuan pinjaman online yang tidak sah, sehingga menimbulkan kekhawatiran terkait keamanan finansial individu. Kebocoran data dapat merusak kepercayaan masyarakat terhadap BPJS Kesehatan, karena orang-orang mungkin mempertanyakan tindakan-tindakan keamanan yang diterapkan untuk menjaga kerahasiaan informasi pribadi mereka. Selain itu, tantangan ekonomi yang signifikan dihadapi Indonesia berasal dari kebocoran data pribadi warganya. Kasus kebocoran data pengguna BPJS ini, telah menyebabkan kerugian negara mencapai sekitar 600 triliun rupiah.

Peretasan dan kebocoran data yang telah terjadi pada BPJS Kesehatan tentu menyerang data pribadi seseorang, yang dimana dalam kaidahnya, data pribadi merupakan sebuah data yang dalam pemanfaatannya harus dilakukan atas persetujuan orang yang bersangkutan. Sehingga, perlindungan atas data pribadi merupakan salah satu bagian dari hak pribadi yang secara tersirat memiliki makna bebas dari segala macam gangguan, termasuk kebocoran data pribadi tersebut oleh pihak yang tidak bertanggung jawab. Secara umum, ketentuan mengenai privasi dan data pribadi dapat ditemukan ketentuannya dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau yang disingkat dengan UU ITE, yang sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Dalam negara konstitusional Indonesia, dimana sesuai dengan UUD Pasal 1 ayat 3 yang berbunyi bahwa indonesia adalah negara hukum, sehingga negara tentu memiliki hak dan kewajiban konstitusional dalam melindungi seluruh warga negara. Kewajiban ini juga telah tertuang dalam pembukaan UUD alinea ke-4 yang menyatakan bahwa negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial. Sehingga, negara memiliki kewajiban yang tertuang dalam bentuk perlindungan data pribadi dan hak pribadi

individu yang krusial untuk dilindungi dan dijaga dari permasalahan terkait kebocoran data-data pribadi.

Dalam menghadapi kasus ini, BPJS Kesehatan telah membentuk sebuah tim khusus bekerja sama dengan Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kemkominfo), serta Telkom untuk melakukan penyelidikan. Kemkominfo juga telah mengundang Direksi BPJS Kesehatan untuk segera memverifikasi dan menguji ulang informasi pribadi yang bocor. Setelah itu, KemKominfo juga menghentikan akun penjual data pribadi di Raid Forum tersebut. Selain itu, KemKominfo juga mengambil langkah-langkah pencegahan untuk mencegah penyebaran data yang lebih luas dengan memutus akses pada tiga tautan, yaitu bayfiles.com, mega.nz, dan anonfiles.com.

KESIMPULAN DAN SARAN

Kasus pelanggaran privasi data di BPJS Kesehatan menyoroti urgensi kebijakan dan langkah-langkah perlindungan data di lembaga pemerintah. Kejadian kebocoran data pribadi pengguna BPJS Kesehatan di Indonesia pada Mei 2021, yang melibatkan informasi pribadi 279 juta warga Indonesia, seperti nama lengkap, nomor identitas, nomor telepon, alamat email, dan alamat rumah, merupakan pelanggaran serius terhadap privasi.

Kejadian ini menegaskan perlunya lembaga publik memiliki kebijakan dan langkah-langkah yang solid dalam melindungi data guna mencegah kejadian serupa. Pemerintah Indonesia telah menginisiasi penyelidikan terkait insiden ini, dan Kementerian Komunikasi dan Informatika berjanji untuk segera mengumumkan keputusan resmi terkait masalah tersebut. Perlindungan data pribadi sangat krusial untuk membangun kepercayaan masyarakat dan menjaga integritas lembaga pemerintah. Oleh karena itu, organisasi sektor publik perlu mengambil tindakan proaktif untuk memastikan keamanan data pribadi dan terus mengevaluasi serta meningkatkan kebijakan serta praktik perlindungan data mereka.

Organisasi publik perlu menjaga daftar data pribadi yang bersifat rahasia dengan cermat dan memastikan bahwa data tersebut dienkripsi baik saat disimpan maupun saat berpindah. Diperlukan penerapan kontrol akses yang ketat dan penyektrian jaringan guna membatasi akses ke data yang bersifat rahasia hanya kepada personel yang berhak. Pelatihan berkala bagi karyawan mengenai praktik terbaik keamanan data perlu diadakan, sambil meningkatkan kesadaran akan resiko pelanggaran data. Seluruh karyawan harus mengikuti pelatihan secara berkala dan wajib terhadap konsep serta taktik perlindungan data agar tetap mendapatkan informasi terkini tentang risiko digital maupun fisik. Kemudian juga diperlukan untuk menciptakan undang-undang dan regulasi yang mengatur penanganan data yang bersifat rahasia serta meningkatkan akuntabilitas lembaga pemerintah dan mitra yang mengumpulkan dan menyimpan data tersebut. Dengan menerapkan langkah-langkah ini, organisasi publik dapat mengurangi risiko pelanggaran data secara signifikan dan mencegah kebocoran data pribadi. Penting untuk terus mengevaluasi dan meningkatkan kebijakan dan praktik perlindungan data agar dapat beradaptasi dengan ancaman dan teknologi yang terus berkembang. Organisasi sektor publik perlu memiliki kebijakan dan langkah - langkah tindakan perlindungan data yang kuat guna mencegah terjadinya kejadian serupa.

Organisasi sektor publik dapat memastikan langkah - langkah keamanan siber mereka dapat dikatakan efektif dengan mengkaji dan memperbaharui kebijakan keamanan yang mereka gunakan dalam menghadapi ancaman yang timbul dan memastikan ketepatannya. Organisasi sektor publik perlu secara berkala memonitor efektivitas dan kelengkapan langkah-langkah keamanan siber mereka untuk memastikan kesesuaian dan kerelevannya. Kemudian diperlukan juga untuk membangun budaya kesadaran keamanan siber di antara karyawan dan stakeholders dalam organisasi tersebut guna memastikan bahwa setiap individu memiliki

pemahaman akan urgensi keamanan siber dan tanggung jawab mereka dalam menjaga kerahasiaan informasi yang sensitif.

Daftar Pustaka

Anggi Anggraeni Kusumoningtyas. (2023). NEXUS PENGAWASAN SIBER SEBAGAI INSTRUMEN KEAMANAN NASIONAL DAN RELEVANSINYA DENGAN DEMOKRASI: PERBANDINGAN BEBERAPA NEGARA. *Jurnal Adhikari*, *2*(3), 416–433. https://doi.org/10.53968/ja.v2i3.80
https://jdihn.go.id/files/804/jurnal%20hukum_2020_706-2263-1-pb.pdf

Dewi, N. K. (2023). Peran Internet dalam Meningkatkan Pembangunan Demokrasi di Kawasan Barat Indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional - Jurnal DPR RI, 11(2), 121-132.

Sindy Ariyaningsih, A. Ari Andrianto, Adri Surya Kusuma, Rezi (2023). KORELASI KEJAHATAN SIBER DENGAN PERCEPATAN DIGITALISASI DI INDONESIA