KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research
Vol.2, No.6 Desember 2024
e-ISSN: 3025-9851; p-ISSN: 3025-986X, Hal 586-593
DOI: https://doi.org/10.61722/jssr.v2i6.2996

Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia

Cinda Sorisa
Universitas Palangka Raya
Cindi Lusia Kiareni
Universitas Paalngka Raya
Jadiaman Parhusip
Universitas Palangka Raya
Program Studi Teknik Teknik Informatika, Fakultas Teknik,Universitas Palangka Raya
Jalan Hendrik Timang, Palangka Raya, Kalimantan Tengah 73111
Korespondensi penulis: sorisacinda13@gemail.com

Abstrak. *This study examines the cyber ethics implications in the 2021 BPJS Kesehatan data breach in Indonesia. It analyzes ethical and technical challenges posed by the incident, in which 279 million participants' sensitive data were leaked and sold online. The research aims to identify the causes, ethical implications, and institutional responsibilities. Using a case study approach, the study highlights the gaps in cybersecurity frameworks and ethical governance in public sector institutions. Findings indicate significant deficiencies in security monitoring, technical safeguards, and ethical accountability. The study recommends enhancing cybersecurity policies, fostering professional ethics, and increasing public trust through institutional transparency and robust data protection practices.*

Keywords: *Cybersecurity; data breach; ethics; personal data protection; public trust.*

Abstrak Penelitian ini membahas implikasi etika keamanan siber dalam kebocoran data BPJS Kesehatan tahun 2021 di Indonesia. Studi ini menganalisis tantangan etika dan teknis yang muncul akibat insiden tersebut, di mana 279 juta data peserta bocor dan dijual secara daring. Penelitian bertujuan mengidentifikasi penyebab, dampak etis, dan tanggung jawab institusional. Dengan pendekatan studi kasus, hasil penelitian menunjukkan kesenjangan dalam kerangka keamanan siber dan tata kelola etika di sektor publik. Temuan mengindikasikan kurangnya pemantauan keamanan, perlindungan teknis yang memadai, dan akuntabilitas etis. Studi ini merekomendasikan penguatan kebijakan keamanan siber, peningkatan etika profesional, serta membangun kepercayaan publik melalui transparansi institusi dan perlindungan data yang lebih kuat.

Kata Kunci: Keamanan siber; kebocoran data; etika; perlindungan data pribadi; kepercayaan publik.

PENDAHULUAN

Dalam era digital, keamanan data pribadi menjadi salah satu isu penting yang perlu mendapat perhatian serius, terutama pada sektor publik yang mengelola informasi sensitif masyarakat. Pentingnya perlindungan data pribadi, khususnya dalam bidang kesehatan, semakin mendalam dengan meningkatnya penggunaan teknologi dalam pengelolaan data. Perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia saat ini belum berjalan maksimal, hal ini ditunjukkan dengan masih banyaknya pelanggaran terhadap penyalahgunaan data pribadi akibat dari semakin berkembangnya penggunaan digital platform yang tidak disertai dengan perlindungan hukum yang memadai (Lesmana et al. 2021).

Dalam hal ini, kebocoran data BPJS Kesehatan menjadi titik permasalahan utama yang harus dianalisis lebih lanjut. Kasus kebocoran data BPJS Kesehatan yang terjadi pada tahun 2021

Received September 30, 2024; Revised Oktober 31, 2024; Desember 02, 2024
* Cinda Sorisa, sorisacinda13@gemail.com

menjadi salah satu contoh nyata bagaimana pelanggaran keamanan siber dapat berdampak besar pada kepercayaan publik dan stabilitas layanan masyarakat. Lebih dari 279 juta data pribadi peserta BPJS Kesehatan, termasuk nama, nomor induk kependudukan (NIK), alamat, nomor telepon, dan data kesehatan, dilaporkan bocor dan diperjualbelikan di forum daring. Perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia saat ini belum berjalan maksimal, hal ini ditunjukkan dengan masih banyaknya pelanggaran terhadap penyalahgunaan data pribadi akibat dari semakin berkembangnya penggunaan digital platform yang tidak disertai dengan perlindungan hukum yang memadai.Terdapat kesenjangan antara kebijakan perlindungan data yang ada dan kenyataan di lapangan. Insiden ini tidak hanya menyoroti kelemahan sistem keamanan, tetapi juga pentingnya tanggung jawab etis dalam pengelolaan data.

Kebocoran data seperti ini memperlihatkan adanya kesenjangan antara kebijakan perlindungan data yang diatur dalam regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP), dengan implementasi teknis di lapangan. Hal ini menjadi tantangan besar bagi organisasi yang mengelola data masyarakat untuk memastikan tidak hanya keamanan teknis, tetapi juga kepatuhan terhadap standar etika dan tanggung jawab profesional.Tugas UU ITE adalah menjamin kelancaran proses pembangunan nasional dan menjamin,melindungi hak-hak pengguna jasa internet dan mengambil Tindakan yang tegas terhadap pelaku *cybercrime*.Berdasarkan sifatnya *cybercrime* termasuk kejahatan tanpa batas (*unlimited crime*),sehingga diperlukan langkah-langkah yang komplek,terintegrasi dan berkelajutan (Zaman et al., 2021). Akibat meningkatnya jumlah pengguna teknologi informasi menyebabkan isu mengenai perlindungan data pribadi menjadi hal yang serius karena penyebarannya dapat dilakukan dengan mudah dan cepat melalui teknologi sehingga menimbulkan risiko kebocoran data pribadi seseorang (Lesmana et al., 2021). Maka dari itu jika terjadi kebocoran data pada suatu instansi maka instansi tersebut haruslah menjadi pihak yang bertanggung jawab penuh akan adanya kebocoran data tersebut. BPJS seharusnya memiliki perlindungan yang baik. Hal ini bisa dilakukan dengan investasi yang lebih besar di bidang keamanan (Indonesiawan et al. 2021).

Penelitian ini bertujuan untuk menganalisis kasus kebocoran data BPJS Kesehatan dari perspektif etika keamanan siber. Dengan pendekatan studi kasus, penelitian ini mengkaji faktor-faktor penyebab kebocoran, dampak etis yang ditimbulkan, dan tanggung jawab moral institusi terkait. Hasil penelitian diharapkan dapat memberikan rekomendasi yang aplikatif untuk meningkatkan keamanan data dan membangun kepercayaan publik melalui penerapan etika profesional yang lebih baik.

KAJIAN TEORITIS

Pengertian Etika Profesi

Dalam buku (“BUKU AJAR ETIKA HUKUM”, 2021). Kata "etika" berasal dari kata Yunani "ethos", yang berarti "dapat dijabarkan kembali" dan berarti "kebiasaan”. Etika dapat didefinisikan sebagai pemikiran tentang hal-hal yang kritis dan dapat diterima secara logis tentang norma-norma. Etika Cyber Law dapat dilihat dalam tindakan seseorang (Tanhela Zein Vitadiar, 2021). Etika adalah bidang yang mempelajari dan menjelaskan tentang hak dan kewajiban yang menunjukkan tindakan yang baik atau buruk. Itu juga dapat menjelaskan tanggung jawab seseorang dan mempengaruhi moral manusia dan komitmen mereka terhadap masyarakat (Tanhela Zein Vitadiar, 2021).

Menurut (Ariadi et al., 2022) Ada beberapa prinsip-pronsip etika profesi, adapun prinsip tersebut yaitu:

a. Prinsip tanggung jawab Seluruh profesional dibidangnya masing-masing wajib menerapkan serta memahami apa saja pekerjaan yang dia kerjakan dan lakukan. Tanggung jawab dari seorang akuntan ataupun bidang lain tidak hanya pada saat berkerja atau bertugas, tetapi juga bertanggung jawab pada hasil kerjanya. Sebagai seseorang yang dianggap profesional harus siap berintegritas dan siap bertanggung jawab. Tanggung jawab yang di emban profesional contohnya menerima dengan baik dan penuh tanggung jawab dari keputusan serta tanggung jawab dari keseluruhan pekerjaan yang dibuat dan tanggung jawab dari pekerjaan yang dilakukan jika berhubungan dengan hidup orang lain dan hidup masyarakat lainnya.
b. Prinsip keadilan Didalam prinsip keadilan, profesional diwajibkan untuk lebih memprioritaskan keadilan dibandingkan pada setiap pekerjaan. Unsur keadilan harus selalu ada untuk setiap Tindakan yang dilaksanakan. Pekerjaannya yang dilakukan buat orang lain diharuskan diberikan. Terutama jika profesional tersebut berkerja dengan hubungan pelayanan terhadap seseorang. Seperti profesi petugas yang berwajib, dokter terhadap pasien, guru terhadap murid dan profesi lain yang melayani orang lain.
c. Prinsip otonomi Maksud dari otonomi ini ialah. Bahwa seorang profesional masihlah memiliki proporsi kebebasannya di dalam pekerjaan. Mereka memiliki hak dan kewajiban yang diperoleh sesuai porsi pekerjaannya. Otonomi ini dilakukan ya atau tidaknya dengan berdasarkan kode etik profesi
d. Prinsip integritas moral Etika profesi didalamnya ada yang Namanya integritas moral. Integritas itu adalah gambaran dan sebab dari tingkatan nilai sebuah kualitas kejujuran serta sebagai prinsip moral profesional terhadap seluruh pekerjaan. Ada beberapa hasl yang wajib profesional ingat dalam memulai pekerjaanya, hal itu ialah mengingat bahwa untuk menjaga diri sendiri, profesi serta menjaga kepentingan publik. Semua yang dijelaskan itu merupakan pengertian.

Etika Keamanan Siber

Etika keamanan siber (*cybersecurity ethics*) adalah cabang etika yang berfokus pada prinsip moral dan tanggung jawab dalam melindungi sistem, data, dan privasi individu dari ancaman siber. Etika memainkan peran penting dalam Cyber security, karena membantu memandu tindakan para profesional dan organisasi dalam dunia digital yang kompleks (Gunawan et al. 2024). Beberapa teori etika utama yang berlaku dalam ilmu komputer meliputi (Munawar et al.2022):

a. Etika Deontologi adalah teori etika yang menekankan pada tindakan itu sendiri, bukan hasil dari tindakan tersebut. Dalam konteks ilmu komputer, deontologi dapat digunakan untuk mengevaluasi tindakan yang dilakukan oleh profesional IT, seperti pengembang perangkat lunak, administrator sistem, dan lainnya, berdasarkan prinsip-prinsip moral dan etika, bukan berdasarkan hasil atau konsekuensi dari tindakan tersebut (Prabhumoye dkk., 2020). Menekankan pentingnya kewajiban moral dalam melindungi data pengguna. Dalam konteks kebocoran data BPJS Kesehatan, institusi memiliki kewajiban mutlak untuk menjaga kerahasiaan dan keamanan data pribadi peserta.
b. Etika Utilitarianisme adalah teori etika yang berfokus pada hasil atau konsekuensi dari tindakan. Menilai keputusan berdasarkan dampaknya terhadap kesejahteraan terbesar bagi banyak orang. Misalnya, kebijakan keamanan siber yang efektif di BPJS Kesehatan dapat mencegah kerugian besar bagi masyarakat.

c. Etika dalam Penggunaan dan Pengelolaan Data Etika dalam penggunaan dan pengelolaan data merujuk pada serangkaian prinsip dan pedoman yang mengatur bagaimana data dikumpulkan, disimpan, diproses, dan digunakan (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016). Dalam era digital saat ini, data telah menjadi aset yang sangat berharga dan penting. Namun, penggunaan dan pengelolaan data yang tidak etis dapat menimbulkan berbagai masalah, termasuk pelanggaran privasi, diskriminasi, dan penyalahgunaan data.
d. Etika Virtue**:** Menitikberatkan pada karakter dan nilai moral para profesional yang bertanggung jawab dalam mengelola sistem keamanan. Profesional teknologi informasi harus memiliki integritas dan komitmen terhadap perlindungan data.
e. Teori Kepercayaan (*Trust Theory)**:*** Dalam keamanan siber, kepercayaan menjadi elemen kunci dalam hubungan antara pengguna dan penyedia layanan. Kebocoran data dapat mengikis kepercayaan publik dan menimbulkan konsekuensi jangka panjang.

Kasus Kebocoran Data BPJS Kesehatan di Indonesia

Pada penelitian sebelumnya Maulida & Utomo (2023) menyatakan bahwa peristiwa kebocoran data pribadi konsumen terjadi pada bulan Mei 2021 lalu, Indonesia dihebohkan dengan dugaan kebocoran data pengguna BPJS Kesehatan sebanyak 279 juta data pribadi pengguna diperjualbelikan di Raid Forums dengan harga jual hingga 80 juta rupiah. Raid Forums merupakan sebuah situs jual-beli seperti marketplace yang menjual-belikan database, atau tentang kebocoran database yang disebabkan oleh hacker. Data tersebut berisikan nomor kartu, data keluarga atau data tanggungan, dan status pembayaran yang identik dengan data yang dikelola oleh Badan Penyelenggaraan Jaminan Sosial (BPJS) Kesehatan (Setiyono, 2002).

Dalam penelitian Oktaviani et al. (2021) menyatakan bahwa kebocoran data BPJS Kesehatan terungkap setelah sebuah akun bernama Kotz yang bertindak sebagai pembeli sekaligus penjual data pribadi (reseller) menawarkannya di sebuah forum daring Raid Forums. Penjual mengklaim memiliki 279 juta salinan data identitas warga Indonesia dengan menunjukkan contoh kurang lebih 100.000 data. Hingga saat ini kasus tersebut masih dalam tahap pemeriksaan forensik digital, dengan begitu korporasi BPJS Kesehatan belum dapat dimintai pertanggungjawabannya, sampai hasilnya diketahui dan unsur deliknya dapat dibuktikan.

Dalam penelitian Nusantara et al. (2024) menjelaskan bahwa kejadian kebocoran data yang ditemui BPJS Kesehatan pada tahun 2021 dengan menggunakan metodologi siklus hidup keamanan, yang terdiri dari tahapan identifikasi, penilaian, perlindungan, dan pemantauan. Hasil pemeriksaan mengungkapkan bahwa kerentanan dalam kerangka keamanan TI dan tidak adanya pemantauan berkelanjutan adalah faktor utama yang berkontribusi terhadap insiden tersebut. Konsekuensi dari pelanggaran data ini patut diperhatikan, menimbulkan ancaman bagi privasi individu dan menodai reputasi BPJS Kesehatan.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode penelitian kepustakaan. Metode ini dipilih untuk mengumpulkan data dan informasi dari berbagai sumber literatur yang relevan dengan topik etika keamanan siber dengan studi kasus kebocoran data BPJS Kesehatan di Indonesia. Penelitian kepustakaan ini dengan menggali berbagai referensi, seperti jurnal ilmiah, buku, artikel, dan sumber-sumber terpercaya lainnya yang membahas isu keamanan siber, kebocoran data, dan perlindungan data pribadi. Data yang diperoleh dari sumber-sumber tersebut akan dianalisis secara kritis untuk mendapatkan pemahaman yang mendalam mengenai penyebab, dampak, dan tanggung jawab etis yang terkait dengan kebocoran data BPJS Kesehatan, dan data yang dikumpulkan akan diidentifikasi menggunakan pola-pola penting yang dapat menjelaskan

permasalahan kebocoran data dan bagaimana isu etika keamanan siber seharusnya diterapkan dalam praktik pengelolaan data pribadi.

HASIL PENELITIAN DAN PEMBAHASAN

Penyebab Kebocoran Data BPJS Kesehatan di Indonesia

Penelitian ini mengidentifikasi sejumlah faktor yang menyebabkan kebocoran data BPJS Kesehatan pada tahun 2021. BPJS Kesehatan, yang dikenal sebagai Badan Penyelenggara Jaminan Soal Kesehatan, didirikan pada tanggal 1 Januari 2014 sebagai bagian dari upaya pemerintah Indonesia untuk menawarkan cakupan kesehatan nasional kepada seluruh masyarakat. Sebelum kejadian signifikan pada Mei 2021,BPJS Kesehatan telah mengalami banyak kasus pelanggaran keamanan data. Pada tahun 2018, ada insiden aksestidak sah di mana data pribadi beberapa peserta dikompromikan. Kejadian ini menggarisbawahi kerentanan dalam infrastruktur keamanan dan pengelolaan data BPJS Kesehatan. Selanjutnya, pada 2019, pelanggaran lain menyebabkan penyebaran data peserta secara tidak sah di internet. Masing-masing episode ini memberikan wawasan berharga tentang pentingnya perlindungan data dan perlindungan privasi peserta, menggarisbawahi perlunya peningkatan berkelanjutan dalam aparat keamanan informasi BPJS Kesehatan(Nusantaraet al. 2024).

Salah satu faktor utama adalah kerentanan dalam kerangka keamanan teknologi informasi (TI) yang digunakan oleh BPJS Kesehatan. Sistem keamanan yang tidak memadai dan tidak adanya pemantauan berkelanjutan membuka celah bagi para pelaku kejahatan siber untuk menyusup. Selain itu, lemahnya implementasi kebijakan keamanan siber dan kurangnya pelatihan bagi staf untuk mengenali ancaman keamanan juga berkontribusi terhadap insiden ini. Kerentanan mendasar yang menyebabkan insiden ini terutama berasal dari kekurangan dalam menerapkan kerangka keamanan siber BPJS Kesehatan. Dampak dari pelanggaran ini sangat mendalam. Informasi pribadi 279 juta orang Indonesia, termasuk data sensitif, kini beredar di internet. Hal ini menghadirkan risiko besar terhadap privasi dan keamanan individu, termasuk potensi penyalahgunaan data untuk kegiatan ilegal seperti pencurian identitas dan pelanggaran keuangan lainnya. (Nusantaraet al. 2024).

Dalam hal terdapat juga faktor eksternal atau faktor luar yang mengakibatkan kebocoran data yang termasuk kejahatan cyber crime atau kejahatan dunia maya. Penyelenggaraan sistem elektronik mengandung resiko yang sangat besar terhadap ancaman-ancaman peretasan yang dilakukan oleh oknum hacker (Peng, 2020). Dalam penelitian Maulida & Utomo (2023) menyatakan Pada kasus kebocoran data pribadi pengguna BPJS Kesehatan, hasil Investigasi menemukan bahwa akun bernama Kotz menjual data pribadi di Raid Forums. Akun Kotz sendiri merupakan pembeli dan penjual data pribadi (reseller). Studi forensik digital yang dilakukan setelah insiden tersebut mengungkapkan bahwa data pribadi sebanyak 279 juta pengguna terpapar dan dijual di forum daring. Situasi ini menunjukkan bahwa perlindungan data pribadi belum menjadi prioritas utama dalam pengelolaan teknologi di BPJS Kesehatan. Setelah terjadinya kebocoran tersebut, BPJS selaku pihak yang mengalami kebocoran data melakukan koordinasi dengan Kementerian Kominfo dan Badan Siber dan Sandi Negara (BSSN) (Indonesiawan et al. 2021).

Dampak Kebocoran Data dari Perspektif Etika

Kebocoran data ini memiliki dampak etis yang serius, baik bagi individu yang datanya bocor maupun bagi institusi BPJS Kesehatan. Dampak dari pelanggaran ini sangat mendalam. Informasi pribadi 279 juta orang Indonesia, termasuk data sensitif, kini beredar di internet. Hal ini menghadirkan risiko besar terhadap privasi dan keamanan individu, termasuk potensi

penyalahgunaan data untuk kegiatan ilegal seperti pencurian identitas dan pelanggaran keuangan lainnya. Selain itu, kedudukan BPJS Kesehatan sebagai penyedia layanan kesejahteraan sosial mengalami konsekuensi yang merugikan (Nusantaraet al. 2024). Kebocoran data pribadi akan berdampak serius terhadap banyak orang yang data pribadinya tersebar luas. Selain privasi terganggu, mereka dapat menjadi korban kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau praktik doxing, yaitu membongkar dan menyebarkan informasi target sasaran oleh pihak-pihak yang tidak berwenang. Kebocoran data bahkan dapat mengganggu stabilitas negara. Kebocoran data penduduk memudahkan pihak manapun secara global untuk melancarkan operasi propaganda komputasional (Zaman et al., 2021).

Dari sudut pandang individu, pelanggaran ini mengakibatkan risiko privasi yang signifikan, seperti pencurian identitas dan potensi eksploitasi data untuk tujuan yang merugikan. Hal ini melanggar prinsip integritas moral dalam etika profesi, di mana institusi harus melindungi hak privasi masyarakat. Di sisi lain, dari perspektif institusi, insiden ini mengikis kepercayaan publik terhadap BPJS Kesehatan sebagai penyedia layanan publik yang andal. Tanggung jawab etis yang diemban BPJS Kesehatan untuk menjaga keamanan data peserta tidak hanya menyangkut aspek teknis, tetapi juga komitmen moral untuk melindungi data dari ancaman siber.

Tanggung Jawab Moral dan Implementasi Keamanan Siber

Berdasarkan analisis, BPJS Kesehatan memiliki tanggung jawab moral dan hukum untuk memastikan data pribadi peserta terlindungi. Prinsip keadilan dalam etika profesi menuntut BPJS Kesehatan untuk mengambil langkah-langkah perbaikan yang transparan, seperti meningkatkan sistem keamanan TI, menerapkan pemantauan berkelanjutan, dan memastikan kepatuhan terhadap peraturan perlindungan data, seperti UU PDP dan UU ITE.

Berdasarkan alineia ke-4 Pembukaan Undang-Undang Dasar Negera republik Indonesia Tahun 1945, dapat disimpulkan bahwa pemerintah Indonesia memiliki peran penting dalam menjaga, mencegah, dan atau menanggulai terjadinya sebuah permasalahan terkait kebocoran data diri rakyatnya baik kebocoran tersebut di akibatkan karena cybercrime maupun tidak pemerintah masih berkewajiban dalam menjaga, mencegah ataupun menanggulagi (Zaman et al., 2021). Investasi pada infrastruktur keamanan yang lebih canggih serta pelatihan berkala bagi staf mengenai ancaman siber sangat diperlukan. Selain itu, pendekatan berbasis etika deontologi menekankan bahwa BPJS Kesehatan harus menjaga data peserta tanpa kompromi, terlepas dari biaya atau kompleksitas teknis.

Rekomendasi untuk Meningkatkan Keamanan Data

Untuk mencegah insiden serupa di masa depan, berikut merekomendasikan langkah-langkah untuk meningkatkan keamanan data berikut:

1. Audit dan evaluasi sistem keamanan secara berkala untuk mengidentifikasi dan memperbaiki kerentanan yang ada.
2. Pendidikan dan Awareness: Menyediakan informasi dan pelatihan mengenai keamanan siber dan etika digital untuk masyarakat. Hal ini bertujuan untuk membantu masyarakatmemahami pentingnya keamanan siber dan bagaimana cara mengatasi ancaman siber dan Pengembangan Kode Etik dengan Menyusun dan mengembangkan kode etik untuk masyarakat, perusahaan, dan institusi terkait keamanan siber(Gunawan et al. 2024).
3. Sosialisasi dan pelatihan keamanan siber bagi seluruh staf BPJS Kesehatan guna meningkatkan kesadaran terhadap ancaman siber. Selain itu, BPJS Kesehatan harus melakukan evaluasi berkala terhadap protokol dan proses keamanan mereka, bersama dengan audit rutin untuk menjamin keamanan sistem yang berkelanjutan. Selain itu, BPJS Kesehatan harus melakukan

evaluasi berkala terhadap protokol dan proses keamanan mereka, bersama dengan audit rutin untuk menjamin keamanan sistem yang berkelanjutan (Nusantaraet al. 2024).

4. Peningkatan transparansi dalam pengelolaan data untuk memulihkan kepercayaan masyarakat, termasuk melibatkan pihak ketiga independen dalam melakukan audit keamanan.
5. Penerapan teknologi enkripsi data untuk memastikan data hanya dapat diakses oleh pihak yang berwenang.

Dengan mengintegrasikan pendekatan teknologi dan etika, BPJS Kesehatan diharapkan mampu membangun sistem perlindungan data yang lebih baik, memberikan jaminan atas hak privasi masyarakat, dan meningkatkan kepercayaan publik terhadap layanan mereka.

KESIMPULAN

Berdasarkan hasil pembahasan kasus kebocoran data BPJS Kesehatan pada tahun 2021 menjadi bukti nyata lemahnya perlindungan data pribadi di Indonesia, yang mengindikasikan adanya celah dalam sistem keamanan siber dan implementasi regulasi terkait. Kebocoran yang melibatkan data sensitif lebih dari 279 juta peserta BPJS ini menimbulkan dampak besar terhadap kepercayaan publik dan privasi individu, termasuk risiko penyalahgunaan data untuk tindakan ilegal.

Dari perspektif etika, insiden ini menekankan pentingnya tanggung jawab moral dan profesional dalam pengelolaan data. Prinsip-prinsip etika profesi seperti tanggung jawab, keadilan, otonomi, dan integritas moral menjadi dasar yang harus diterapkan dalam sistem keamanan siber oleh organisasi seperti BPJS Kesehatan. Selain itu, pendekatan etika utilitarianisme dan deontologi menunjukkan perlunya kebijakan yang tidak hanya berfokus pada hasil, tetapi juga pada kewajiban melindungi data pribadi peserta secara etis dan menyeluruh.

Sebagai langkah perbaikan, institusi seperti BPJS Kesehatan harus mengadopsi strategi keamanan siber yang lebih tangguh, termasuk peningkatan teknologi, pelatihan staf, dan pemantauan sistem secara berkelanjutan. Selain itu, penting untuk memperkuat penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan mengintegrasikan langkah-langkah penegakan hukum yang efektif. Upaya ini diharapkan dapat memitigasi risiko kebocoran data di masa depan dan membangun kembali kepercayaan masyarakat terhadap layanan publik.

DAFTAR PUSTAKA

Ariadi, D., Husna, G. A., & Budiwitjaksono, G. S. (2022). Analisis etika profesi dalam era digitalisasi pada kantor akuntan publik. Jurnal Ilmiah MEA (Manajemen, Ekonomi, Dan Akuntansi), 6(2).

Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1), 154-167.

Indonesiawan, R. C. S., Alroy, M., Suci, T. L., & Prasetyo, B. R. (2021). Analisis Privasi Data Pengguna Dalam Instansi Bpjs Kesehatan. In *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* (Vol. 1, No. 1, pp. 174-182).

Lesmana, CT, Elis, E., & Hamimah, S. (2021). Urgensi UU Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak privasi masyarakat Indonesia. *Jurnal Rechten: Penelitian Hukum dan Hak Asasi Manusia* , *3* (2), 1-6.

Maulida, O., & Utomo, H. (2023). Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan atas kebocoran data pribadi pengguna dalam perspektif hukum pidana. *Indonesian Journal of Law and Justice*, *1*(2), 10-10.

Munawar, Z., Kom, M., Heryana, N., Riza, B. S., Ma'sum, H., Setiadi, A., ... & Yayasan, P. ETIKA DALAM ILMU KOMPUTER.

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan. *Nuansa Informatika*, *18*(2), 120-127.

Oktaviani, S., Dewata, Y. J., & Fadlian, A. (2021). Pertanggung Jawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE. *De Juncto Delicti: Journal Of Law*, *1*(2), 146-157.

Prabhumoye, S., Boldt, B., Salakhutdinov, R., & Black, A. W. (2020). Case study: Deontological ethics in NLP. arXiv preprint arXiv:2010.04658.

Peng, X. (2020). Analysis of Magnetic-Flux Leakage (MFL) Data for Pipeline Corrosion Assessment. IEEE Transactions on Magnetics, 56(6). https://doi.org/10.1109/TMAG.2020.2981450

Tanhela Zein Vitadiar, dkk. (2021). BUKU AJAR ETIKA HUKUM CYBER . CV. AE MEDIA GRAFIKA.

Zaman, A. A., Anwar, J., & Fadlian, A. (2021). "Pertanggung Jawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE."