ANALISIS KEPATUHAN ETIKA PROFESI DAN KEAMANAN SISTEM: STUDI KASUS KEBOCORAN DATA BPJS KESEHATAN

Stevani Dean Safira[1], Retno Purwani Setyaningrum[2], Nanda Rosma Anwar[3], Medistra Aldrin[4], Ilham Maulana Cakra Dwi Noto[5], Muhammad Alwi Nur Fathihah[6]

[1,2,3,4,5,6]Universitas Pelita Bangsa
Jalan. Inspeksi Kalimalang Tegal Danas Arah Deltamas, Cibatu, Cikarang

Email : [1]stevanidean312110463@mhs.pelitabangsa.ac.id , [2]retno.purwaningrum@pelitabangsa.ac.id, [3]nandarosma2004@gmail.com, [4]medistra37@gmail.com, [5]maulana.312110027@mhs.pelitabangsa.ac.id, [6]alwi.16@mhs.pelitabangsa.ac.id

ABSTRAK

Kebocoran data menjadi ancaman yang semakin meningkat seiring pesatnya perkembangan teknologi informasi. Penelitian ini mengkaji hubungan antara kepatuhan etika profesi dan penerapan keamanan sistem dalam kasus kebocoran data di Indonesia. Dengan pendekatan kualitatif, penelitian ini menganalisis faktor-faktor penyebab kebocoran data, baik dari aspek perilaku manusia maupun kelemahan teknologi. Penelitian ini menyelidiki apakah kebocoran data lebih sering terjadi karena kelalaian menerapkan etika profesi atau karena sistem keamanan yang tidak memadai. Analisis dilakukan dalam kerangka regulasi nasional, terutama Undang-undang Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa kebocoran data umumnya disebabkan oleh kombinasi faktor manusia dan teknologi, dengan kurangnya kepatuhan pada standar keamanan dan rendahnya kesadaran etika sebagai faktor dominan. Penelitian ini menyarankan perlunya strategi yang lebih efektif untuk meningkatkan kesadaran dan kepatuhan terhadap standar keamanan, serta dapat menjadi dasar pengembangan kebijakan pencegahan kebocoran data di masa depan.

Kata kunci: *Etika Profesi, Keamanan, Tanggung Jawab, Kebocoran Data, Kepatuhan*

ABSTRACT

Data breaches have become an increasingly prevalent threat alongside the rapid development of information technology. This research examines the relationship between compliance with professional ethics and the implementation of system security in data breach cases in Indonesia. Using a qualitative approach, this study analyzes the causal factors of data breaches, both from human behavioral aspects and technological vulnerabilities. The research investigates whether data breaches more frequently occur due to negligence in applying professional ethics or because of inadequate security systems. The analysis is conducted within the framework of national regulations, particularly the Personal Data Protection Law. Research findings indicate that data breaches are generally caused by a combination of human and technological factors, with lack of compliance with security standards and low ethical awareness as dominant factors. This research suggests the need for more effective strategies to increase awareness and compliance with security standards, and can serve as a foundation for developing policies to prevent data breaches in the future.

Keywords: *Professional Ethics, Security, Responsibility, Data Breach, Compliance.*

1. PENDAHULUAN

Kebocoran data pribadi menjadi salah satu ancaman serius di era digital, hal ini menunjukkan adanya celah besar dalam penerapan etika profesi dan keamanan sistem. Teknologi informasi telah membawa banyak kemudahan, tetapi juga memperbesar risiko apabila tidak diimbangi dengan tanggung jawab etis dan teknis. Terutama ketika melibatkan instansi layanan publik yang menyimpan jutaan data diri masyarakat [1]. Oleh karena itu, etika menjadi peran penting sebagai prinsip moral yang mengatur perilaku dan tindakan manusia. Etika dapat juga dipahami sebagai pemikiran tentang hal-hal yang kritis dan rasional terhadap norma-norma yang berlaku [2]. Dalam keamanan data, Etika Keamanan Siber 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 [3].

Permasalahan muncul ketika prinsip-prinsip etika ini tidak diimplementasikan secara maksimal, terutama dalam pengelolaan sistem informasi dan data pribadi. Kasus BPJS Kesehatan pada tahun 2021 silam menjadi salah satu kasus menggemparkan publik dan menyoroti lemahnya kepatuhan terhadap etika profesi serta celah pada sistem keamanan informasi [4]. Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan merupakan bentuk Badan Hukum Milik Negara (BHMN) yang berfungsi menyelenggarakan program jaminan kesehatan.

Pada konteks ini, kebocoran data BPJS Kesehatan yang terjadi pada tahun 2021 menjadi topik yang menarik untuk dibahas dan diteliti lebih lanjut, sebab pada tahun 2021 undang-undang perlindungan data pribadi (UU PDP) belum ada, sehingga yang dirugikan 100% adalah pengguna atau masyarakat itu sendiri, sedangkan pemegang data dan pemroses data, yaitu instansi pemerintah dan industri swasta, mereka tidak memiliki risiko yang terlalu tinggi [5]. Pandemi covid yang terjadi pada 2019 merupakan salah satu faktor tertundanya pengesahan UU PDP ini, dikarenakan pada saat itu fokus pemerintahan lebih tertuju kepada penanganan pandemi, pemulihan ekonomi, serta legislasi terkait pandemi [6].

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 [1]. Pakar digital forensik Rubby Alamsyah membenarkan bahwa kebocoran data pada BPJS Kesehatan terjadi karena pemberian akses data kepada pihak ketiga atau vendor. Namun, Rubby mengungkapkan bahwa pemberian akses tersebut tidak diikuti dengan pemantauan dan audit yang ketat. Sehingga hal ini dapat dinilai bahwa pengelolaan data oleh pemerintah tidak memikirkan aspek keamanan dan terkesan meremehkan.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis tingkat kepatuhan[7], terhadap etika profesi dan penerapan keamanan sistem informasi dalam kasus kebocoran data BPJS Kesehatan. Dengan pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih menyeluruh mengenai akar permasalahan serta upaya yang dapat dilakukan untuk mencegah kejadian serupa di masa mendatang.

2. TINJAUAN PUSTAKA

2.1 Etika Profesi

Etika Profesi "Etika" berasal dari kata Yunani "*ethos*", yang berarti "dapat dijabarkan kembali" dan "kebiasaan". Jadi, etika dapat didefinisikan sebagai pemikiran tentang hal-hal yang kritis dan dapat diterima secara logis tentang norma-norma yang telah ditetapkan. Secara umum, etika adalah nilai-nilai moral yang mendasari tindakan seseorang dan membuatnya dapat dipercaya [3]. Sebagai praktisi profesi, penerapan dan pelaksanaan etika profesi sangat penting jika kita ingin bekerja dengan baik dan menjaga kepercayaan masyarakat terhadap layanan yang kita berikan [2]. Dalam melakukan setiap pekerjaan, etika profesi sangat berkaitan dengan sikap dan sifat profesional dan profesionalisme. Etika profesi adalah sikap hidup yang adil untuk memberikan pelayanan profesional kepada masyarakat dengan penuh ketertiban dan keahlian sebagai pelayanan dalam rangka melaksanakan tugas sebagai kewajiban terhadap masyarakat [8].

2.2 Keamanan Sistem

Keamanan informasi merupakan aspek krusial yang mencakup perlindungan informasi dan sistem informasi dari berbagai bentuk ancaman tidak sah. Secara komprehensif, keamanan informasi didefinisikan sebagai upaya melindungi aset informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, maupun penghancuran oleh pihak yang tidak memiliki otoritas, dengan tujuan utama menjaga aspek kerahasiaan, integritas, dan kemudahan penggunaan [2]. Perlu dipahami bahwa keamanan informasi bukanlah konsep tunggal, melainkan integrasi dari berbagai elemen yang mencakup organisasi, sumber daya manusia, proses operasional, serta infrastruktur teknologi.

Dalam paradigma keamanan informasi kontemporer, terdapat tiga aspek fundamental yang menjadi pilar utama dalam pengelolaan dan pengendalian keamanan sistem informasi. Aspek pertama adalah

Kerahasiaan (*Confidentiality*) yang berfungsi sebagai mekanisme kontrol untuk memastikan bahwa informasi hanya dapat diakses oleh individu atau entitas yang memiliki otorisasi resmi. Aspek kedua, Integritas (*Integrity*), berperan sebagai penjamin bahwa data tidak mengalami manipulasi tanpa persetujuan pihak berwenang, sehingga keakuratan dan keutuhan informasi tetap terjaga. Aspek ketiga yaitu Ketersediaan (*Availability*) merupakan jaminan bahwa sistem dan data dapat diakses dan digunakan pada waktu dan lokasi sesuai kebutuhan pengguna yang memiliki otorisasi.

2.3 Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan

Pemerintah Indonesia mendirikan Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yang merupakan bagian dari Sistem Jaminan Sosial Nasional (SJSN), untuk meningkatkan kesehatan dan kesejahteraan masyarakat. Tugas BPJS Kesehatan adalah menjalankan program jaminan sosial kesehatan nasional [9]. Sesuai dengan mandat yang diatur dalam Undang-Undang No. 40 Tahun 2004 tentang SJSN dan Undang-Undang No. 24 Tahun 2011 tentang BPJS, program BPJS Kesehatan bertujuan untuk memastikan bahwa setiap warga negara Indonesia memiliki hak yang setara untuk mendapatkan layanan kesehatan.

Transformasi dari PT Askes (Persero) menjadi BPJS Kesehatan dimulai sejak 2004, dan resmi ditetapkan pada 2011. Melalui program Kartu Indonesia Sehat, BPJS Kesehatan memastikan perlindungan kesehatan komprehensif bagi seluruh masyarakat Indonesia [10].

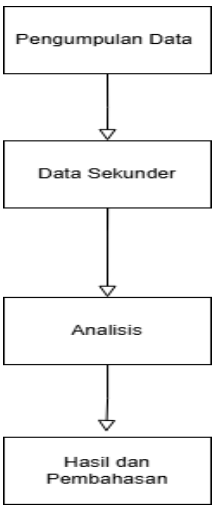
Sebagai penyelenggara Program Jaminan Kesehatan Nasional-Kartu Indonesia Sehat (JKN-KIS), BPJS Kesehatan berpartisipasi dalam perkembangan teknologi informasi yang cepat berubah. Melalui aplikasi Mobile JKN, BPJS Kesehatan mulai memberikan berbagai kemudahan, kepraktisan, dan kecepatan dari layanan fisik ke layanan jaringan. Aplikasi Mobile JKN, yang pertama kali dirilis pada tahun 2017, terus dikembangkan dan diperbaharui dengan tujuan meningkatkan kepuasan peserta. Fitur-fitur baru ini membuatnya lebih mudah bagi peserta JKNKIS untuk mengakses layanan kesehatan, menyelesaikan berbagai keperluan administrasi.

Fasilitas kesehatan yang bekerja sama dengan BPJS Kesehatan harus terakreditasi untuk meningkatkan pelayanan dan menjaga keselamatan pasien peserta JKN-KIS. Baik itu Fasilitas Kesehatan Tingkat Pertama (FKTP), seperti puskesmas, klinik pratama, dan dokter praktik perorangan, maupun Fasilitas Kesehatan Rujukan Tingkat Lanjutan (FKRTL), seperti rumah sakit dan klinik utama. Hal ini sesuai dengan Permenkes 71 Tahun 2023 tentang Pelayanan Kesehatan pada Jaminan Kesehatan Nasional dan Peraturan Menteri Kesehatan nomor 3 Tahun 2023, yang memperbaiki tarif pelayanan kesehatan peserta program JKN, baik tarif kapitasi maupun non kapitasi, dan INA CBGs. Perbaikan tarif ini diharapkan meningkatkan pelayanan kesehatan.

Pada Juni 2023, program (KESSAN), yang merupakan proses evaluasi pelayanan yang dilakukan oleh BPJS Kesehatan melalui mekanisme survei untuk mengumpulkan umpan balik atau kesan pengalaman peserta setelah menerima layanan dari Fasilitas Kesehatan, dan program Supervisi Buktikan dan Lihat Langsung (Sibling), yang merupakan proses evaluasi pelayanan yang dilakukan oleh BPJS Kesehatan melalui mekanisme survei untuk mengumpulkan umpan balik atau kesan pengalaman peserta setelah menerima layanan dari Fasilitas Kesehatan.

3. METODE PENELITIAN

Kajian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Data bersifat sekunder, diperoleh dari kutipan pakar dan pernyataan resmi yang disampaikan dalam konferensi atau forum publik terkait kebocoran data di Indonesia. Fokus analisis terletak pada aspek etika profesi dan tanggung jawab lembaga dalam menjamin keamanan sistem informasi. Kajian ini juga menelaah respons serta langkah yang diambil oleh pihak terkait dalam menangani insiden kebocoran data, dengan studi kasus pada kebocoran data BPJS Kesehatan yang dijual secara ilegal di platform daring seperti Raid Forums.



Gambar 1. Alur pengumpulan data

Proses pengambilan data kualitatif dalam penelitian ini dilakukan melalui pemanfaatan data sekunder dengan tahapan sistematis sebagaimana diilustrasikan pada Gambar 1. Diagram alur berikut menunjukkan rangkaian prosedur yang diterapkan dalam pengumpulan, seleksi, dan pengolahan data sekunder untuk memperoleh informasi yang relevan dengan fokus penelitian. Teknik pengumpulan data dilakukan dengan metode dokumentasi dan studi literatur, yang mencakup pengumpulan berita, laporan resmi, kutipan dari juru bicara instansi terkait, serta referensi akademik yang mendukung. Seluruh dokumen tersebut kemudian dianalisis menggunakan pendekatan analisis tematik, yaitu dengan cara mengelompokkan data ke dalam tema-tema utama seperti pelanggaran etika, kelalaian sistem keamanan, dan bentuk penanganan insiden.

Pengolahan data dilakukan dengan pendekatan analisis tematik [10], yang diawali dengan proses pemilahan dan seleksi terhadap dokumen yang relevan. Selanjutnya, isi data dikelompokkan berdasarkan dimensi etika profesi dan sistem keamanan informasi. Interpretasi dilakukan secara naratif untuk menemukan keterkaitan antara temuan dokumen dengan teori-teori etika dan keamanan informasi. Hasil interpretasi digunakan sebagai dasar dalam merumuskan kesimpulan akhir mengenai kepatuhan serta efektivitas penanganan kasus kebocoran data yang dianalisis. Dengan pendekatan ini, diharapkan penelitian mampu memberikan gambaran kritis dan menyeluruh mengenai kepatuhan terhadap prinsip etika profesi serta efektivitas penanganan kebocoran data dalam konteks keamanan digital di Indonesia.

4. PEMBAHASAN

4.1 Kronologi Kasus Kebocoran Data BPJS Kesehatan 2021

Menurut Artikel dari Tempo. Pada Mei 2021, Indonesia mengalami musibah dengan kebocoran data peserta BPJS Kesehatan yang mencakup sekitar 279 juta warga. Kebocoran ini pertama kali ketahuan setelah akun bernama "Kotz" di forum RaidForums menawarkan satu juta sampel data untuk diperjual belikan. Data yang bocor ini mencakup informasi sensitif meliputi nama lengkap, Nomor Induk Kependudukan (NIK), tanggal lahir, alamat, nomor telepon, dan bahkan beberapa data kesehatan terkait [4].

Dalam menanggapi kasus kebocoran data BPJS Kesehatan, pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo) serta Badan Siber dan Sandi Negara (BSSN). Menurut Juru Bicara Kominfo, Dedi Permadi mengungkapkan bahwa *Raid Forums* teridentifikasi sebagai forum yang banyak menyebarkan konten yang melanggar perundang-undangan di Indonesia, sehingga situs tersebut sedang dilakukan proses pemblokiran [11]. Sedangkan pihak BPJS sendiri tidak langsung mengakui kebocoran ini, hanya saja mengakui adanya kesamaan antara data yang bocor dengan data yang mereka kelola. Menteri Koordinator Bidang Pembangunan Manusia dan Kebudayaan, Muhadjir Effendy, menyatakan bahwa dugaan kebocoran data BPJS Kesehatan masih dalam tahap investigasi, dan belum dapat dipastikan keasliannya. Ia juga menegaskan bahwa layanan BPJS Kesehatan tetap berjalan normal dan tidak terdampak oleh dugaan insiden tersebut [12].

4.2 Analisis Penyebab Kebocoran Data

4.2.1 Menurut Sisi Teknologi

Dari sisi teknologi, sistem penyimpanan data BPJS Kesehatan dinilai memiliki sistem pertahanan data yang buruk, dan apabila data tersebut bocor maka data-data itu dapat dengan mudah digunakan oleh pihak yang tidak bertanggung jawab. “Tentunya dugaan kebocoran data yang diduga dari BPJS Kesehatan tersebut, bila dikaitkan dengan banyaknya aplikasi di BPJS Kesehatan maka kebocoran data tersebut kemungkinan bisa disebabkan diretasnya aplikasi-aplikasi tersebut khususnya aplikasi Sistem Informasi Manajemen Kepesertaan dan aplikasi pelayanan kesehatan,” kata Koordinator Advokasi BPJS Watch Timboel Siregar dalam keterangannya [13].

4.3 Regulasi perlindungan Data Pribadi

Dalam konteks perlindungan data pribadi, regulasi utama yang menjadi acuan di Indonesia adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini secara resmi disahkan untuk memberikan dasar hukum yang kuat terkait hak individu atas data pribadinya serta kewajiban pengendali dan prosesor data dalam menjaga keamanan informasi tersebut. Dalam kasus kebocoran data BPJS Kesehatan yang terjadi pada tahun 2021, regulasi ini memang belum berlaku, sehingga mekanisme perlindungan hukum terhadap korban menjadi sangat lemah. UU PDP mengatur prinsip-prinsip perlindungan data seperti keabsahan pemrosesan data, perlunya persetujuan subjek data, hak akses, hak koreksi, hingga hak untuk menghapus data (*right to be forgotten*). Selain itu, pengendali data diwajibkan untuk melaporkan insiden kebocoran data kepada otoritas dalam jangka waktu tertentu. Studi oleh E. Aulia dalam jurnal Unes Law Review juga menegaskan bahwa keberadaan UU PDP membawa kepastian hukum dalam perlindungan data pribadi di Indonesia [6]. Dengan diberlakukannya UU PDP, diharapkan kejadian serupa seperti kasus BPJS Kesehatan dapat diminimalisir di masa depan melalui penerapan standar keamanan informasi yang lebih ketat dan adanya sanksi hukum terhadap pihak yang lalai.

4.4 Dampak Kebocoran Data

Kebocoran data ini memiliki dampak yang luas terhadap masyarakat. Masyarakat sebagai pemilik data yang bocor berisiko menjadi korban kejahatan yang memanfaatkan data pribadi mereka. Masyarakat juga menghadapi risiko doxing (pembocoran informasi pribadi) dan ancaman psikologis akibat penyalahgunaan data medis dan berpotensi dimanfaatkan untuk kejahatan finansial, seperti peminjaman ilegal atau pembukaan rekening fiktif [14]. Kepercayaan masyarakat pun menurun karena merasa bahwa data mereka tidak dikelola dengan aman, kekecewaan ini benar-benar disayangkan karena menyebabkan ketidakpercayaan masyarakat terhadap kinerja pemerintah dalam menangani data pribadi masyarakat. Hingga sekarang survei oleh Lembaga Studi Keamanan Siber Indonesia (LSKSI) pada 2025 menunjukkan bahwa 67% korban kebocoran data mengalami penurunan kepercayaan terhadap layanan publik [15].

4.5 Penanganan yang Dilakukan

Menurut artikel dari Cloud Computing Indonesia, Kementerian Komunikasi dan Informatika (Kominfo) melakukan pemblokiran situs Raid Forums dan akun bernama ‘Kotz’. Menurut mereka mengambil langkah ini cukup efektif untuk mencegah semakin meluasnya data yang bocor. ada pula yang mereka umumkan Kominfo kembali memblokir situs BreachForums dan platform terkait, sementara BSSN melakukan penetration testing (uji penetrasi) terhadap sistem BPJS Kesehatan untuk mengidentifikasi kerentanan baru. “Kedua tim dalam proses insiden respons secara tuntas guna meyakinkan pelaku tidak menanam backdoor sehingga tetap memiliki akses ke sistem, lalu memastikan data yang di eksfiltrasi oleh pelaku dan sistem elektronik lain yang mungkin terdampak, dan melakukan atribusi pelaku untuk keperluan penegakan hukum,” tutur Juru Bicara BSSN, Anton Setiawan melansir dari Tempo, Senin (24/5/2021). Kominfo juga melakukan pemblokiran terhadap tiga tautan yang digunakan untuk mengunduh data pribadi yang bocor tersebut, yaitu bayfiles.com, mega.nz, dan anonfiles.com untuk mengantisipasi kebocoran lebih jauh[16].

5. KESIMPULAN

Penelitian ini menunjukkan bahwa kebocoran data BPJS Kesehatan pada tahun 2021 disebabkan oleh kombinasi kelemahan sistem teknologi dan kelalaian manusia, terutama dalam hal kepatuhan terhadap etika profesi dan standar keamanan informasi. Minimnya kesadaran etis serta lemahnya pengawasan terhadap akses data menjadi faktor dominan dalam terjadinya insiden tersebut. Dampak dari kebocoran ini sangat merugikan masyarakat sebagai pemilik data, termasuk risiko penyalahgunaan data pribadi dan menurunnya kepercayaan terhadap layanan publik. Oleh karena itu, diperlukan peningkatan kesadaran etika profesi, penguatan kebijakan keamanan data, serta penerapan sistem pengawasan yang lebih ketat sebagai langkah preventif terhadap insiden serupa di masa depan.

DAFTAR PUSTAKA

[1] R. Milafebina, I. P. Lesmana, dan M. R. Syailendra, "Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia," *J. Tana Mana*, vol. 4, no. 1, hlm. 157–169, 2023.

[2] F. Pritama, E. R. D. Leluni, dan J. Parhusip, "Analisis Pelanggaran Etika Profesi Keamanan Siber (Studi Kasus Kebocoran Data Pajak di Indonesia)," *Tek. J. Ilmu Tek. Dan Inform.*, vol. 4, no. 2, hlm. 53–56, 2024.

[3] C. Sorisa, C. L. Kiareni, dan J. Parhusip, "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia," *J. Sains Stud. Res.*, vol. 2, no. 6, hlm. 586–593, 2024.

[4] R. C. S. Indonesiawan, M. Alroy, T. L. Suci, dan B. R. Prasetyo, "ANALISIS PRIVASI DATA PENGGUNA DALAM INSTANSI BPJS KESEHATAN," *Pros. Semin. Nas. Teknol. Dan Sist. Inf.*, vol. 1, no. 1, hlm. 174–182, 2021.

[5] K. R. Anggen Suari dan I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, hlm. 132–142, Apr 2023, doi: 10.38043/jah.v6i1.4484.

[6] E. Aulia, "Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dari Perspektif Kepastian Hukum," *Unes Law Rev.*, vol. 7, no. 1, hlm. 220–227, 2024.

[7] N. I. Febrianto dan L. Kartikasari, "Pengaruh Teknik Audit Berbantuan Komputer (TABK) terhadap Kualitas Audit dengan Prosedur Audit sebagai Variabel Moderasi," *J. Akunt. Indones.*, vol. 13, no. 1, hlm. 54–66, 2024.

[8] K. Sobon, "ETIKA TANGGUNG JAWAB EMMANUEL LEVINAS," *J. Filsafat*, vol. 28, no. 1, hlm. 47, Feb 2018, doi: 10.22146/jf.31281.

[9] S. Nurul, Shynta Anggrainy, dan Siska Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, hlm. 564–573, Mei 2022, doi: 10.31933/jemsi.v3i5.992.

[10] H. Heriyanto, "Thematic Analysis sebagai Metode Menganalisa Data untuk Penelitian Kualitatif," *Anuva*, vol. 2, no. 3, hlm. 317, Nov 2018, doi: 10.14710/anuva.2.3.317-324.

[11] O. Maulida dan H. Utomo, "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna dalam Perspektif Hukum Pidana," *Indones. J. Law Justice*, vol. 1, no. 2, hlm. 10, Des 2023, doi: 10.47134/ijlj.v1i2.2011.

[12] M. R. Faiqy, M. I. Damargara, M. Alhidayah, dan J. Maulana, "Urgensi Realisasi Peran Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi," *Padjadjaran Law Rev.*, vol. 10, no. 1, Jul 2022, doi: 10.56895/plr.v10i1.838.

[13] A. Hermawan, "Mengintip Celah antara Potensi dan Tantangan Big Data pada Layanan Jaminan Sosial Ketenagakerjaan Indonesia," *J. Jamsostek*, vol. 2, no. 2, hlm. 185–206, Jun 2024, doi: 10.61626/jamsostek.v2i2.59.

[14] N. A. Alfitri, R. Rahmawati, dan F. Firmansyah, "Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *J. Soc. Soc.*, vol. 4, no. 2, hlm. 92–111, Des 2024, doi: 10.54065/jss.4.2.2024.511.

[15] F. Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *AL-BAHTS J. Ilmu Sos. Polit. Dah Huk.*, vol. 2, no. 1, hlm. 8–16, Jan 2024, doi: 10.32520/albahts.v2i1.3044.

[16] M. A. T. Dzaky dan I. F. Edrisy, "Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital," *PESHUM J. Pendidik. Sos. Dan Hum.*, vol. 4, no. 2, hlm. 3614–3625, 2025, doi: https://doi.org/10.56799/peshum.v4i2.8311.