Keamanan Data dan Pencurian Identitas Digital: Studi Kasus BPJS Kesehatan dari Perspektif Teknologi Informasi dan Hukum Pidana

Data Security and Digital Identity Theft: A Case Study of BPJS Health from the Perspective of Information Technology and Criminal Law

Ismaya Dewi Priyani[1], Yogi Abdullah[2], Novita Anggraini[3], Harry Pribadi Fitrian[4], Winda Sulastri[5]

[1]Hukum,[2]DKV, [3,4,5]Informatika, Universitas Teknologi Digital, Bandung, Indonesia,
Email correspondensi: ismayapriyani@digitechuniversity.ac.id

Info Artikel

Riwayat Artikel:
Diajukan: 01/05/2025
Diterima: 02/05/2025
Diterbitkan: 27/08/2025

Kata Kunci:
Data, Keamanan, Digital, Informasi, Statistik

Keyword:
Data, Security, Digital, Information, Statistics

https://doi.org/

A B S T R A K

Perkembangan internet yang pesat mempermudah akses informasi, namun juga meningkatkan risiko kebocoran data pribadi. Prinsip perlindungan data menekankan pembatasan penggunaan data dan kewajiban menjaga keamanan dari risiko kehilangan, akses, modifikasi, atau penyalahgunaan tanpa izin. Lembaga publik seperti BPJS Kesehatan wajib memastikan pengelolaan data peserta sesuai prinsip ini, termasuk pengawasan terhadap pihak ketiga. Kebocoran data BPJS Kesehatan yang melibatkan jutaan peserta menimbulkan risiko pencurian identitas digital dan potensi penipuan. Analisis teknologi informasi menunjukkan kelemahan pada enkripsi, kontrol akses, audit internal, dan integrasi API dengan pihak ketiga sebagai faktor penyebab kebocoran. Perspektif hukum pidana menegaskan kewajiban BPJS berdasarkan UU Perlindungan Data Pribadi (UU PDP 2022) dan UU ITE 2008, meskipun kasus ini belum memiliki putusan hakim inkrah. Penelitian ini menggunakan pendekatan deskriptif kualitatif menggabungkan analisis TI dan hukum pidana. Hasil menunjukkan perlunya strategi pencegahan yang komprehensif, termasuk penguatan sistem TI, literasi digital, kepatuhan hukum, dan kolaborasi lintas sektor. Studi ini menekankan bahwa keamanan data merupakan tanggung jawab institusi dan aspek krusial untuk membangun ekosistem digital publik yang aman dan terpercaya.

A B S T R A C T

The rapid development of the Internet has facilitated access to information but also increased the risk of personal data breaches. Data protection principles emphasize the restriction of data usage and the obligation to maintain security against risks such as loss, unauthorized access, modification, or misuse. Public institutions such as BPJS Health are required to ensure that the management of participant data complies with these principles, including monitoring third-party involvement. The BPJS Health data breach, which involved millions of participants, poses risks of digital identity theft and potential fraud. Information technology analysis indicates weaknesses in encryption, access control, internal audits, and API integration with third parties as contributing factors to the breach. From a criminal law perspective, BPJS has obligations under the Personal Data Protection Law (PDP Law 2022) and the Electronic Information and Transactions Law (ITE Law 2008), although this case has not yet reached a final court decision. This study uses a qualitative descriptive approach combining IT and criminal law analysis. The results highlight the need for a comprehensive prevention strategy, including strengthening IT systems, digital literacy, legal compliance, and cross-sector collaboration. The study emphasizes that data security is an institutional responsibility and a crucial aspect of building a safe and trustworthy public digital ecosystem.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital berlangsung sangat pesat. Internet tidak hanya menjadi sarana komunikasi dan hiburan, tetapi juga memudahkan akses informasi, layanan publik, dan transaksi ekonomi. Layanan digital yang semakin meluas, termasuk sistem kesehatan elektronik seperti BPJS Kesehatan, membawa kemudahan besar bagi masyarakat. Namun, kemajuan ini juga membuka peluang bagi tindakan kriminal baru yang dikenal sebagai kejahatan siber, khususnya pencurian data dan identitas digital. Kejahatan siber memiliki karakteristik yang berbeda dengan kejahatan konvensional. Tidak hanya menimbulkan kerugian finansial, tetapi juga berpotensi merusak reputasi lembaga dan mengancam keamanan data pribadi masyarakat. Di Indonesia, penetrasi internet yang tinggi lebih dari 77% populasi pada 2024 menjadi peluang sekaligus risiko bagi lembaga publik yang mengelola data pribadi jutaan orang. BPJS Kesehatan, sebagai penyelenggara sistem elektronik publik, mengelola data sensitif yang mencakup nama, NIK, nomor kartu, tanggal lahir, alamat, dan informasi kesehatan peserta [3]. Kebocoran data di sistem ini akan berdampak luas, mulai dari pencurian identitas hingga penipuan finansial. Prinsip dasar perlindungan data pribadi menekankan bahwa data hanya boleh digunakan sesuai tujuan yang telah ditentukan, dan tidak boleh diakses, diungkapkan, atau dimodifikasi tanpa izin pemilik data atau pihak berwenang sesuai hukum. Selain itu, prinsip keamanan wajar mengharuskan penyelenggara sistem elektronik menjaga data dari risiko kehilangan, akses ilegal, perusakan, modifikasi, dan penyalahgunaan. Dalam konteks BPJS, hal ini menjadi tanggung jawab institusi sebagai penyelenggara sistem elektronik publik, yang harus memastikan pengelolaan data sesuai UU Perlindungan Data Pribadi (UU PDP 2022) dan UU ITE 2008 [6],[7], serta melakukan pengawasan ketat saat bekerja sama dengan pihak ketiga. Artikel ini menghubungkan tiga aspek utama: pertama, analisis teknologi informasi, termasuk kelemahan sistem TI internal, enkripsi, kontrol akses, dan integrasi pihak ketiga; kedua, perspektif hukum pidana, meninjau kewajiban dan potensi sanksi berdasarkan UU PDP dan UU ITE; ketiga, dampak sosial-ekonomi, termasuk risiko pencurian identitas digital, penurunan kepercayaan masyarakat, dan potensi kerugian finansial. Dengan kerangka ini, artikel berusaha memberikan gambaran menyeluruh tentang bagaimana kebocoran data BPJS terjadi, faktor penyebabnya, dan strategi mitigasi yang diperlukan untuk membangun sistem digital publik yang aman dan terpercaya berkelanjutan. Selain itu pentingnya privasi menyadarkan kita perlunya menyoroti pentingnya pemahaman yang lebih mendalam tentang harapan dan kebutuhan pengguna dalam pengelolaan privasi di media sosial serta kebutuhan akan langkah-langkah lebih lanjut untuk meningkatkan kesadaran, keamanan, dan perlindungan privasi bagi pengguna di platform-platform media sosial tersebut [1].

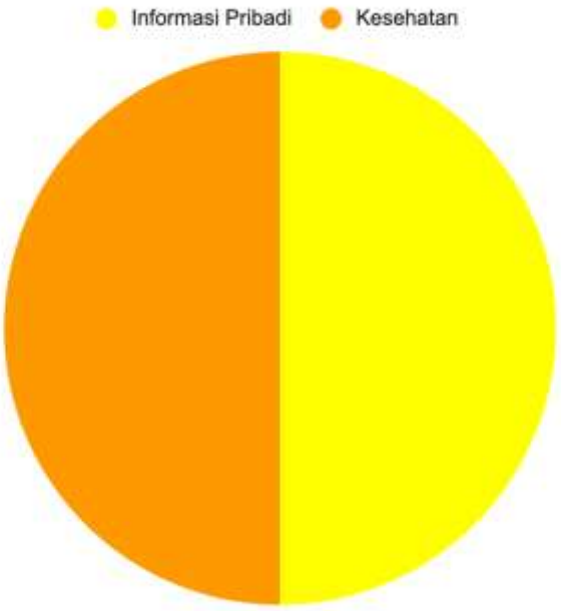
2. METODE PELAKSANAAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dan statistik deskriptif yang merupakan deskripsi yang berkenaan dengan deskripsi data [2], menggabungkan analisis teknologi informasi dan hukum pidana dengan pengolahan data statistik deskriptif. Pendekatan ini dipilih karena kebocoran data BPJS Kesehatan melibatkan aspek teknis TI, regulasi hukum, dan dampak sosial-ekonomi. Sumber data berasal dari laporan resmi BPJS Kesehatan, Kominfo, BSSN, APJII, serta literatur akademik terkait keamanan siber dan hukum pidana. Analisis TI fokus pada kelemahan sistem, seperti kontrol akses, enkripsi, audit internal, dan integrasi pihak ketiga. Analisis hukum menelaah kewajiban BPJS berdasarkan UU PDP 2022 dan UU ITE 2008, termasuk potensi sanksi bila terjadi kelalaian. Data dianalisis secara naratif untuk menyusun kronologi kebocoran, menilai faktor penyebab, mengevaluasi dampak sosial-ekonomi, dan merumuskan strategi pencegahan. Pendekatan ini memberikan gambaran menyeluruh tentang fenomena kebocoran data dan solusi yang dapat diterapkan untuk memperkuat keamanan data publik.

3. HASIL DAN PEMBAHASAN

Kasus kebocoran data BPJS Kesehatan menjadi sorotan penting dalam ranah keamanan informasi dan perlindungan data di Indonesia. Dengan jumlah peserta yang mencapai ratusan juta, data yang dikelola mencakup informasi pribadi dan kesehatan yang sangat sensitif, sehingga kerentanannya berimplikasi luas terhadap hukum, sosial, dan ekonomi. Fenomena ini menunjukkan bahwa meskipun institusi publik memiliki sistem TI modern, celah keamanan tetap dapat dimanfaatkan pihak yang tidak bertanggung jawab, menimbulkan risiko pencurian identitas dan penipuan finansial. Pembahasan berikut

akan menyoroti kronologi kebocoran, analisis kelemahan sistem TI, perspektif hukum pidana, dampak sosial-ekonomi, serta strategi mitigasi dan pencegahan untuk memperkuat keamanan data publik.



Gambar 1. Data Penelitian

3.1 Kronologi Kebocoran Data BPJS Kesehatan

Kebocoran data BPJS Kesehatan pertama kali terungkap ke publik pada Mei 2021, ketika informasi jutaan peserta muncul di forum online yang dapat diakses secara bebas. Data yang bocor mencakup nama lengkap, Nomor Induk Kependudukan (NIK), nomor kartu BPJS, tanggal lahir, alamat, nomor telepon, dan alamat email. Jenis informasi ini sangat sensitif karena dapat dimanfaatkan untuk pencurian identitas, penipuan finansial, dan akses ilegal ke layanan digital.

BPJS awalnya menepis kabar kebocoran tersebut, namun investigasi dari pakar keamanan siber dan peneliti independen membuktikan bahwa kebocoran memang terjadi. Sebagian data berasal dari database internal BPJS, sementara sebagian lainnya diambil melalui penggabungan informasi publik yang tersedia melalui pihak ketiga. Analisis menunjukkan bahwa data dapat diunduh secara massal tanpa terdeteksi, menandakan kelemahan sistem dan pengawasan internal.

Beberapa faktor teknis menjadi penyebab utama kebocoran. Pertama, kontrol akses internal yang longgar memungkinkan pihak tidak berwenang mengakses data sensitif. Kedua, enkripsi data tidak diterapkan secara menyeluruh, sehingga sebagian informasi dapat diakses dengan relatif mudah. Ketiga, audit internal dan monitoring sistem belum optimal, sehingga aktivitas pengambilan data massal tidak terdeteksi sejak awal. Keempat, integrasi API dengan pihak ketiga dilakukan tanpa protokol keamanan yang memadai, meningkatkan risiko kebocoran data.

Kejadian ini menegaskan bahwa meskipun BPJS telah menerapkan sistem TI modern, kombinasi kelemahan teknis dan pengawasan yang minim membuka celah bagi pihak tidak bertanggung jawab. Kebocoran data ini memiliki implikasi serius, baik dari sisi hukum, sosial, maupun ekonomi, karena menyangkut jutaan warga Indonesia. Insiden ini menjadi bukti pentingnya penguatan sistem TI, penerapan audit internal yang ketat, serta kepatuhan penuh terhadap UU Perlindungan Data Pribadi (UU PDP 2022) dan UU ITE 2008.

3.2 Analisis Teknologi Informasi dan Hukum Pidana

Kebocoran data BPJS Kesehatan menunjukkan bahwa keamanan sistem informasi publik bukan hanya masalah teknis, tetapi juga memiliki konsekuensi hukum yang signifikan di era digital. Dari perspektif teknologi informasi, salah satu

kelemahan utama terletak pada kontrol akses internal yang longgar, di mana hak akses dan peran pengguna tidak dibedakan secara ketat. Kondisi ini memungkinkan pihak internal maupun pihak ketiga mengekstraksi data secara massal tanpa terdeteksi. Kelemahan ini berkaitan langsung dengan kewajiban hukum yang diatur dalam Pasal 47 UU Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, yang mewajibkan Penyelenggara Sistem Elektronik menjaga keamanan data pribadi dengan langkah teknis dan administratif memadai. Kegagalan menjaga kontrol akses dapat menimbulkan sanksi pidana atau administratif bagi pihak yang bertanggung jawab.

Penerapan enkripsi data yang belum menyeluruh meningkatkan risiko kebocoran informasi sensitif. Data yang tidak terenkripsi atau hanya sebagian terenkripsi mudah diakses oleh pihak yang tidak berwenang, sehingga dapat dimanfaatkan untuk pencurian identitas, penipuan finansial, atau penyebaran informasi ilegal. Dalam konteks hukum pidana, hal ini diatur oleh Pasal 30 dan 31 UU ITE 2008, yang melarang pengaksesan dan penyebaran informasi elektronik tanpa izin. Dengan demikian, kelemahan teknis terkait enkripsi langsung berpotensi menimbulkan tindak pidana jika data bocor atau disalahgunakan.

Audit internal dan monitoring sistem yang kurang optimal juga menjadi faktor krusial. Aktivitas pengambilan data dalam jumlah besar kerap tidak terdeteksi karena mekanisme early warning system belum efektif. Di era digital, serangan siber semakin canggih melalui teknik otomatisasi atau kecerdasan buatan (AI), sehingga kelemahan ini membuka peluang kebocoran massal yang sulit dikendalikan. Dalam perspektif hukum, kelalaian dalam mendeteksi atau mencegah akses ilegal dapat menimbulkan tanggung jawab pidana atau administratif, sesuai Pasal 48 UU PDP.

Integrasi sistem BPJS dengan pihak ketiga melalui API tanpa protokol keamanan yang memadai menambah risiko tambahan. UU PDP menegaskan bahwa penyelenggara sistem tetap bertanggung jawab atas pengelolaan data pribadi, termasuk ketika bekerja sama dengan pihak eksternal. Pelanggaran kewajiban ini dapat dikualifikasi sebagai kelalaian atau perbuatan pidana jika menimbulkan kerugian atau data digunakan secara ilegal.

Dari perspektif hukum pidana secara khusus, BPJS Kesehatan sebagai Penyelenggara Sistem Elektronik publik memiliki tanggung jawab untuk menjaga keamanan data peserta. Pasal 26 ayat (1) UU PDP menyatakan bahwa setiap penyelenggara sistem elektronik wajib memproses data pribadi sesuai tujuan yang telah ditetapkan dan memperoleh persetujuan pemilik data. Pasal 47 ayat (1) menegaskan kewajiban menjaga keamanan data dengan langkah teknis dan administratif yang memadai untuk mencegah kebocoran, akses ilegal, atau penyalahgunaan. Sementara itu, Pasal 48 UU PDP menyebutkan sanksi pidana dan administratif bagi pihak yang lalai atau sengaja melakukan pelanggaran, termasuk denda dan kemungkinan hukuman penjara.

UU ITE Nomor 11 Tahun 2008 juga relevan, terutama Pasal 30 dan 31, yang melarang pengaksesan dan penyebaran informasi elektronik secara ilegal. Jika pihak internal atau pihak ketiga mengambil, menyebarkan, atau memanfaatkan data tanpa izin, tindakan tersebut dapat dipidana berdasarkan UU ITE. Hingga saat ini, kasus kebocoran BPJS belum memiliki putusan hakim yang inkrah, tetapi secara hukum, BPJS memiliki tanggung jawab penuh untuk memastikan pengelolaan data peserta sesuai UU PDP dan UU ITE. Kegagalan menjaga keamanan data dapat menimbulkan konsekuensi pidana bagi individu atau institusi yang lalai, sekaligus membuka peluang klaim hukum dari peserta yang dirugikan.

Secara keseluruhan, insiden kebocoran BPJS menegaskan bahwa aspek teknologi dan hukum tidak dapat dipisahkan. Kelemahan teknis seperti kontrol akses longgar, enkripsi tidak lengkap, audit internal dan monitoring yang lemah, serta integrasi pihak ketiga yang tidak aman, semuanya dapat menimbulkan risiko hukum pidana. Strategi penguatan harus bersifat holistik, mencakup penerapan enkripsi menyeluruh, penguatan kontrol akses, audit dan monitoring real-time, serta kepatuhan penuh terhadap UU PDP dan UU ITE agar sistem TI publik lebih aman dan risiko pelanggaran hukum dapat diminimalkan.

3.3. Strategi Pencegahan Kebocoran Data BPJS

Upaya pencegahan kebocoran data BPJS Kesehatan harus dilakukan secara komprehensif dengan memadukan aspek teknologi informasi, prosedur internal, dan kepatuhan hukum. Dari sisi teknologi, BPJS perlu menerapkan enkripsi menyeluruh untuk seluruh data pribadi peserta, baik yang disimpan di server internal maupun yang ditransmisikan melalui jaringan publik. Enkripsi ini harus menggunakan standar terkini agar data tetap aman meski diakses oleh pihak yang tidak berwenang. Selain itu, kontrol akses berbasis peran harus ditegakkan dengan ketat, memastikan setiap pengguna hanya memiliki hak akses sesuai kebutuhan pekerjaannya. Pemisahan peran (*segregation of duties*) juga perlu dilakukan untuk mencegah penyalahgunaan data oleh pihak internal.

Selain itu, audit internal *dan monitoring real-time* menjadi langkah penting untuk mendeteksi aktivitas mencurigakan sebelum kebocoran terjadi. Penggunaan sistem deteksi dini (*early warning system*) berbasis kecerdasan buatan dan analisis pola akses dapat mengidentifikasi anomali, seperti pengunduhan data dalam volume besar atau akses dari lokasi yang tidak biasa. Penerapan protokol keamanan pada integrasi pihak ketiga termasuk API dan penyedia layanan eksternal, juga harus dilakukan, dengan ketentuan bahwa pihak eksternal tunduk pada standar keamanan dan audit berkala. Berikut strategi preventif dalam bentuk visual.

Gambar 2. Strategi Preventif Agar Terhindar dari Serangan Siber [5]

Kebocoran data BPJS Kesehatan menunjukkan bahwa pengelolaan data publik yang melibatkan jutaan peserta memiliki risiko tinggi apabila sistem teknologi informasi tidak dilengkapi dengan kontrol yang ketat. Faktor utama kebocoran meliputi kelemahan kontrol akses internal, penerapan enkripsi yang belum menyeluruh, audit internal dan monitoring yang kurang optimal, serta integrasi pihak ketiga tanpa protokol keamanan memadai. Dari perspektif hukum pidana, BPJS Kesehatan memiliki kewajiban untuk menjaga keamanan data peserta sesuai UU Perlindungan Data Pribadi (UU PDP 2022) dan UU ITE (2008), dan kelalaian dalam menjalankan kewajiban ini dapat menimbulkan sanksi pidana maupun administratif. Dampak sosial-ekonomi dari kebocoran data ini cukup signifikan, termasuk risiko pencurian identitas, penipuan finansial, dan menurunnya kepercayaan masyarakat terhadap layanan publik digital. Oleh karena itu, upaya pencegahan harus dilakukan secara holistik, dengan memperkuat sistem TI, meningkatkan literasi digital staf internal dan pihak ketiga, menerapkan prosedur operasional standar yang ketat, serta membangun kerja sama lintas lembaga untuk memitigasi risiko kebocoran di masa depan. Secara keseluruhan, studi ini menegaskan bahwa keamanan data merupakan tanggung jawab institusi publik dan merupakan aspek krusial dalam membangun ekosistem digital yang aman, terpercaya, dan berkelanjutan.

4. KESIMPULAN

Penulis mengucapkan terima kasih kepada Universitas Teknologi Digital atas dukungan fasilitas penelitian dan akses data yang memungkinkan terlaksananya penelitian ini. Ucapan terima kasih juga disampaikan kepada BPJS Kesehatan, BSSN, Kominfo, dan APJII atas informasi dan laporan yang menjadi sumber data penting bagi analisis. Penulis menghargai bantuan para pakar keamanan siber dan rekan akademisi yang telah memberikan masukan konstruktif dalam penyusunan artikel ini. Dukungan moral dan ilmiah dari keluarga serta rekan kerja juga sangat berperan dalam kelancaran penelitian dan penyusunan naskah ini.

5. SARAN

Dalam penerapannya, tentu data musti di perkuat dengan analisis yang lebih baik, dengan begitu hasil juga akan lebih baik.

6. DAFTAR PUSTAKA

[1] A. Sriyani, F. Faturahman, Z. Isnan, dan Darsiti, "Survei Kesejahteraan Digital Dalam Pengelolaan Privasi Di Media Sosial," *ITech J. Inf. Syst. Inform.*, vol. 1, no. 1, hlm. 14–18, 2024.

[2] I. D. Priyani dan N. Anggraini, "Survei Jenis Tindak Kejahatan Cyber dalam Lingkungan Universitas di Indonesia," *ITech J. Inf. Syst. Inform.*, vol. 1, no. 1, hlm. 28–35, 2024.

[3] BPJS Kesehatan. (2021). Laporan Kebocoran Data Peserta BPJS Kesehatan. Jakarta: BPJS Kesehatan.

[4] Kominfo. (2024). Statistik Penetrasi Internet dan Keamanan Data di Indonesia. Jakarta: Kementerian Komunikasi dan Informatika.

[5] BSSN. (2024). Laporan Kejahatan Siber Nasional. Jakarta: Badan Siber dan Sandi Negara.

[6] UU Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

[7] UU Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

[8] APJII. (2024). Laporan Survei Pengguna Internet Indonesia. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

[9] Kaspersky Lab. (2022). Data *Breach Analysis and Cybersecurity Recommendations*. Moscow: *Kaspersky Security Reports.*

[10] Whitman, M. E., & Mattord, H. J. (2021*). Principles of Information Security* (6th ed.). Boston: *Cengage Learning.*

[11] Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law* (6th ed.). New York: Wolters Kluwer.