

Strategi Komunikasi Krisis BKN dalam Kasus Dugaan Kebocoran Data ASN

ARDI ARUPA KEWANGGA, FIRDAUS NOOR, FITRIA AYUNINGTYAS

Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional “Veteran” Jakarta, Indonesia
Email: 2510422023@mahasiswa.upnvj.ac.id

Abstrak

Penelitian ini menganalisis strategi komunikasi krisis Badan Kepegawaian Negara (BKN) dalam merespons dugaan kebocoran data Aparatur Sipil Negara (ASN) tahun 2024. Penelitian menggunakan pendekatan kualitatif dengan desain studi kasus dan analisis isi kualitatif terhadap satu siaran pers resmi BKN dan pemberitaan dari tiga media nasional pada fase awal krisis. Analisis dilakukan dengan mengintegrasikan Situational Crisis Communication Theory (SCCT) dan Image Repair Theory (IRT). Hasil penelitian menunjukkan bahwa BKN membingkai insiden sebagai dugaan yang masih dalam proses investigasi, mengimbau pembaruan kata sandi, menegaskan keberlanjutan layanan manajemen ASN, serta menonjolkan koordinasi dengan lembaga terkait. Dalam perspektif SCCT, respons tersebut mencerminkan *instructing information*, *adjusting information*, *diminish*, dan *bolstering*, sedangkan dalam perspektif IRT menunjukkan *reducing offensiveness* dan *corrective action*. Integrasi kedua teori menunjukkan pola stabilisasi institusional dalam kondisi ketidakpastian atribusi, ketika organisasi berupaya menjaga kontinuitas layanan dan reputasi sementara status serta tanggung jawab krisis belum terkonfirmasi secara final. Temuan ini menegaskan fungsi komplementer SCCT dalam mendiagnosis atribusi krisis dan IRT dalam menjelaskan pengelolaan reputasi.

Kata Kunci: BKN; Image Repair Theory; Kebocoran Data; Komunikasi Krisis; SCCT

Abstract

This study analyzes the crisis communication strategies employed by Indonesia's National Civil Service Agency (BKN) in responding to the alleged 2024 data breach involving civil servants (ASN). The study adopts a qualitative case study design and qualitative content analysis of one official BKN press release and news coverage from three national media outlets during the initial phase of the crisis. Situational Crisis Communication Theory (SCCT) and Image Repair Theory (IRT) are integrated as analytical frameworks. The findings show that BKN framed the incident as an allegation under investigation, advised users to update their passwords, emphasized the continuity of civil service management services, and highlighted coordination with relevant institutions. From an SCCT perspective, the response reflects instructing information, adjusting information, diminish, and bolstering, while IRT identifies reducing offensiveness and corrective action. The integration of both frameworks reveals a pattern of institutional stabilization under attributional uncertainty, in which the organization seeks to maintain service continuity and institutional reputation while the status and responsibility for the crisis remain unresolved. The findings demonstrate the complementary roles of SCCT in diagnosing crisis attribution and IRT in explaining reputational management.

Keywords: BKN; Crisis Communication; Data Breach; Image Repair Theory; SCCT

CoverAge

Journal of Strategic
Communication

Vol. 17, No. 1, Hal. 122-146

September 2026.

Fakultas Ilmu Komunikasi,
Universitas Pancasila

Accepted June 20, 2026

Revised August 12, 2026

Approved September 30, 2026

PENDAHULUAN

Transformasi digital telah mengubah cara negara bekerja, berkomunikasi, dan memberikan pelayanan kepada masyarakat. Dalam konteks pemerintahan, data tidak lagi hanya berfungsi sebagai arsip administratif, tetapi telah menjadi bagian dari infrastruktur strategis yang menopang pelayanan publik, koordinasi antarlembaga, serta pengambilan keputusan. Di Indonesia, intensitas penggunaan internet dan media sosial yang terus meningkat menunjukkan bahwa berbagai aktivitas sosial, ekonomi, dan pemerintahan berlangsung dalam ekosistem digital yang semakin padat dan saling terhubung. DataReportal mencatat bahwa pada awal 2024 Indonesia memiliki sekitar 185,3 juta pengguna internet dan 139 juta pengguna media sosial atau sekitar 49,9% dari total populasi (DataReportal, 2024). Kondisi tersebut memperlihatkan semakin kuatnya ketergantungan masyarakat dan institusi terhadap sistem digital. Pada saat yang sama, meningkatnya digitalisasi juga memperbesar kerentanan terhadap berbagai risiko keamanan informasi.

Dalam lingkungan digital yang memungkinkan informasi diproduksi, disebarluaskan, dan diperdebatkan secara cepat oleh media, organisasi, komunitas, maupun individu, isu negatif dapat berkembang menjadi krisis dalam waktu singkat (Estaswara & Anggraeni, 2018). Dengan demikian, digitalisasi menghadirkan

peluang efisiensi sekaligus risiko reputasional yang harus dikelola oleh organisasi.

Salah satu risiko yang semakin menonjol dalam transformasi digital adalah kebocoran data. Persoalan ini menjadi semakin penting ketika insiden melibatkan lembaga pemerintah yang mengelola data dalam jumlah besar. Perlindungan data pribadi dalam konteks pemerintahan tidak dapat dipahami hanya sebagai persoalan keamanan teknologi, tetapi juga berkaitan dengan hak warga, tanggung jawab institusional, dan legitimasi penyelenggaraan pemerintahan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa pelindungan data pribadi merupakan keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data guna menjamin hak konstitusional subjek data. Undang-undang tersebut juga mengatur hak subjek data serta kewajiban pihak yang mengendalikan dan memproses data pribadi (Republik Indonesia, 2022). Oleh karena itu, ketika sebuah lembaga pemerintah menghadapi dugaan kebocoran data, persoalan yang muncul bukan hanya mengenai kemampuan teknis mengamankan sistem, tetapi juga kemampuan institusi menjelaskan situasi, memberikan perlindungan informasi kepada pihak terdampak, dan mempertahankan kepercayaan terhadap tata kelola data yang dilakukannya.

Dalam konteks tersebut, Badan Kepegawaian Negara (BKN) memiliki posisi

yang strategis karena menjadi salah satu lembaga yang berperan dalam pengelolaan data Aparatur Sipil Negara (ASN). Fungsi pengelolaan data ASN mencakup pengelolaan, sinkronisasi, penjaminan kualitas, interoperabilitas, dan penyajian informasi ASN (BKN, 2025). Selain itu, kebijakan Satu Data ASN menekankan bahwa data ASN harus akurat, mutakhir, terpadu, dapat dipertanggungjawabkan, serta dapat dibagipakaikan antarinstansi sesuai prinsip tata kelola data (BKN, 2022). Posisi tersebut menjadikan isu keamanan data di lingkungan BKN memiliki implikasi yang lebih luas daripada persoalan teknis internal. Dugaan gangguan terhadap data ASN berpotensi menimbulkan pertanyaan mengenai kemampuan institusi dalam menjaga informasi yang dikelolanya sekaligus memengaruhi reputasi organisasi sebagai salah satu pengelola utama infrastruktur data birokrasi nasional.

Urgensi tersebut terlihat ketika pada Agustus 2024 muncul informasi mengenai dugaan kebocoran data ASN yang dikaitkan dengan BKN. Pemberitaan media menyebut adanya dugaan penjualan jutaan data ASN melalui forum peretas BreachForums (Kompas, 2024; Tempo, 2024). Menanggapi perkembangan tersebut, BKN menerbitkan Siaran Pers Nomor 007/RILIS/BKN/VIII/2024 pada 11 Agustus 2024. Dalam siaran pers tersebut, BKN menyatakan sedang melakukan identifikasi dan investigasi bersama Badan Siber dan Sandi Negara (BSSN) serta

Kementerian Komunikasi dan Informatika (Kominfo) terhadap isu dugaan kebocoran data ASN. BKN juga menegaskan bahwa dugaan gangguan tersebut tidak berdampak pada layanan manajemen ASN serta mengimbau seluruh pengguna layanan untuk melakukan pembaruan kata sandi secara berkala (BKN, 2024). Respons tersebut memperlihatkan beberapa orientasi komunikasi yang muncul secara bersamaan, yaitu pengakuan terhadap adanya isu yang perlu ditangani, pemberian instruksi keamanan kepada pengguna, penegasan kontinuitas layanan, serta penonjolan koordinasi dengan institusi yang memiliki kewenangan di bidang keamanan siber.

Situasi tersebut memperlihatkan karakter khas krisis siber. Pada fase awal insiden, organisasi sering kali harus berkomunikasi ketika fakta teknis mengenai sumber, skala, maupun tanggung jawab terhadap insiden belum sepenuhnya terkonfirmasi. Sementara proses investigasi membutuhkan waktu, informasi mengenai dugaan insiden dapat berkembang lebih cepat melalui pemberitaan media dan ruang digital. Kondisi ini menciptakan ketegangan antara kebutuhan institusi untuk berhati-hati dalam mengeluarkan pernyataan dan kebutuhan pemangku kepentingan untuk memperoleh informasi yang cepat, jelas, dan dapat digunakan untuk mengurangi risiko. Dengan demikian, komunikasi dalam krisis siber tidak hanya berkaitan dengan penyampaian fakta, tetapi juga dengan bagaimana organisasi

mengelola ketidakpastian dan atribusi tanggung jawab ketika penyebab krisis masih diperdebatkan.

Dimensi atribusi menjadi penting karena ancaman reputasi dalam suatu krisis tidak hanya ditentukan oleh besarnya kerusakan yang terjadi, tetapi juga oleh sejauh mana pemangku kepentingan menempatkan tanggung jawab kepada organisasi. Situational Crisis Communication Theory (SCCT) menjelaskan bahwa atribusi tanggung jawab memengaruhi tingkat ancaman reputasional yang dihadapi organisasi dan menjadi dasar dalam menentukan strategi respons krisis (Coombs, 2007). SCCT membedakan krisis ke dalam kategori *victim crisis*, *accidental crisis*, dan *preventable crisis*, yang masing-masing merepresentasikan tingkat tanggung jawab organisasi yang berbeda. Dalam konteks dugaan kebocoran data, klasifikasi tersebut menjadi kompleks. Di satu sisi, lembaga dapat diposisikan sebagai korban apabila kebocoran berasal dari tindakan eksternal seperti peretasan. Di sisi lain, sebagai pengelola data, lembaga tetap dapat menghadapi atribusi tanggung jawab apabila pemangku kepentingan menilai bahwa sistem keamanan atau tata kelola data seharusnya mampu mencegah insiden tersebut.

Kompleksitas atribusi tersebut menjadikan kasus kebocoran data berbeda dari krisis dengan penyebab dan tanggung jawab yang telah terkonfirmasi secara jelas. Organisasi tidak hanya harus mengelola fakta mengenai insiden, tetapi juga harus mengelola

cara tanggung jawab atas peristiwa tersebut dikonstruksi. Dalam kasus BKN, penggunaan istilah “dugaan kebocoran” dan penekanan bahwa proses identifikasi serta investigasi masih berlangsung menunjukkan bahwa posisi institusional mengenai status insiden belum bersifat final. Sementara itu, pemberitaan media menonjolkan klaim mengenai jumlah data yang diduga bocor, jenis informasi pribadi yang terpapar, harga penjualan data, serta kemungkinan validitas sebagian data (Antara, 2024; Kompas, 2024; Tempo, 2024). Perbedaan tersebut bukan berarti pemberitaan media dapat diperlakukan sebagai representasi langsung atas persepsi publik, tetapi menunjukkan adanya konstruksi media mengenai tingkat keseriusan insiden yang dapat berbeda dari penekanan yang digunakan dalam komunikasi resmi institusi.

Selain persoalan atribusi, krisis juga menghadirkan ancaman terhadap citra organisasi. Image Repair Theory (IRT) menjelaskan bahwa ketika suatu organisasi dikaitkan dengan tindakan atau peristiwa yang berpotensi merusak reputasi, organisasi dapat menggunakan berbagai strategi diskursif untuk mempertahankan atau memulihkan citranya (Benoit, 1997). Strategi tersebut mencakup *denial*, *evasion of responsibility*, *reducing offensiveness*, *corrective action*, dan *mortification*. Kerangka IRT memberikan perhatian yang lebih spesifik terhadap bagaimana organisasi membangun pesan ketika reputasinya berada dalam ancaman. Oleh karena itu, jika SCCT membantu

menjelaskan hubungan antara atribusi tanggung jawab, tingkat ancaman reputasi, dan pilihan respons krisis, IRT memungkinkan analisis yang lebih rinci terhadap fungsi reputasional dari pesan yang digunakan organisasi.

Sejumlah penelitian terdahulu menunjukkan bahwa komunikasi menjadi bagian penting dalam penanganan krisis kebocoran data. Diers-Lawson et al. (2021) menunjukkan bahwa kemampuan organisasi menghadapi kebocoran data berkaitan dengan hubungan pemangku kepentingan dan kapasitas komunikasi strategis. Penelitian Nguyen et al. (2024) memperlihatkan bahwa framing media terhadap krisis organisasi dapat membentuk cara sebuah peristiwa dipresentasikan dalam ruang publik. Sementara itu, Chen et al. (2022) menunjukkan pentingnya strategi pemulihan kepercayaan setelah insiden keamanan dalam konteks layanan berbasis digital. Temuan yang lebih mutakhir dari Choi et al. (2025) juga menunjukkan bahwa respons terhadap krisis kebocoran data berkaitan dengan upaya pemulihan kepercayaan pada organisasi pemerintah, organisasi profit, maupun nonprofit. Literatur tersebut memperlihatkan bahwa kebocoran data bukan semata persoalan gangguan teknis, tetapi merupakan peristiwa reputasional yang menuntut organisasi mengelola hubungan dengan pemangku kepentingan, komunikasi risiko, dan kepercayaan.

Dalam konteks Indonesia, kajian

mengenai kebocoran data dan komunikasi krisis juga terus berkembang, meskipun fokusnya masih tersebar dalam beberapa pendekatan. Febriandy dan Wahyutama mengkaji strategi komunikasi pemerintah dalam kasus Pusat Data Nasional Sementara melalui perspektif IRT. Penelitian tersebut menempatkan strategi pemulihan citra sebagai salah satu fokus utama dalam membaca respons pemerintah terhadap krisis data (Febriandy & Wahyutama, 2025). Maulana dan Nasrulloh (2024) menggunakan perspektif pemulihan citra untuk menganalisis respons Bank Syariah Indonesia setelah dugaan serangan siber. Tannavaro dan Wiraguna (2025) menyoroti strategi komunikasi humas dalam krisis siber melalui kasus BPJS Kesehatan dan Bank Syariah Indonesia. Sementara itu, Nurhayati dan Laksmi (2023) menunjukkan bagaimana pemberitaan media membingkai kebocoran data aplikasi PeduliLindungi. Kajian lain menempatkan kebocoran data dalam kerangka perlindungan hukum dan kepatuhan keamanan (Panggabean & Fitria, 2025; Safira et al., 2025). Adapun Najib (2023) telah mengkaji komunikasi krisis BKN, tetapi dalam konteks kecurangan seleksi CASN dan bukan krisis kebocoran data.

Kajian-kajian tersebut memberikan landasan penting untuk memahami komunikasi krisis siber, tetapi sekaligus menunjukkan adanya persoalan akademik yang masih memerlukan penjelasan. Literatur yang digunakan dalam penelitian ini

memperlihatkan kecenderungan analisis yang menitikberatkan pada salah satu dimensi, seperti pemulihan citra, *framing media*, komunikasi institusional, atau aspek tata kelola dan perlindungan data. Dalam kondisi tersebut, hubungan antara bagaimana tanggung jawab terhadap krisis dikonstruksi dan bagaimana organisasi mengelola konsekuensi reputasional dari konstruksi tersebut belum banyak dijelaskan secara simultan, terutama dalam konteks lembaga pemerintah yang menghadapi dugaan kebocoran data ketika investigasi teknis masih berlangsung. Persoalannya dengan demikian bukan sekadar belum banyaknya penelitian mengenai BKN sebagai objek, melainkan adanya kebutuhan untuk menjelaskan bagaimana atribusi tanggung jawab dan strategi pengelolaan reputasi bekerja secara bersamaan pada fase awal krisis yang ditandai oleh ketidakpastian.

Atas dasar persoalan tersebut, penelitian ini mengintegrasikan SCCT dan IRT bukan sekadar sebagai dua perangkat klasifikasi strategi komunikasi, melainkan sebagai dua kerangka analisis yang bekerja pada tingkat berbeda dan saling melengkapi. SCCT digunakan untuk mendiagnosis bagaimana krisis dikonstruksi, bagaimana tingkat tanggung jawab organisasi diposisikan, serta strategi respons apa yang digunakan dalam menghadapi ancaman reputasional. IRT selanjutnya digunakan untuk membaca bagaimana pesan yang muncul dalam respons tersebut menjalankan fungsi

mempertahankan atau memperbaiki citra organisasi. Dengan konstruksi ini, analisis tidak berhenti pada pernyataan bahwa suatu pesan merupakan *instructing information*, *diminish*, atau *corrective action*, tetapi diarahkan untuk menjelaskan hubungan antara ketidakpastian atribusi, pilihan respons, dan pengelolaan reputasi institusional.

Integrasi kedua kerangka tersebut menjadi penting dalam kasus BKN karena fase awal krisis menunjukkan adanya ketidakpastian mengenai status dan tanggung jawab atas dugaan kebocoran data. BKN belum mengafirmasi secara final bahwa kebocoran telah terjadi, tetapi pada saat yang sama melakukan investigasi, memberikan instruksi protektif, menegaskan keberlanjutan layanan, dan menunjukkan koordinasi dengan institusi terkait. Kombinasi pesan tersebut membuka ruang analisis mengenai bagaimana lembaga pemerintah berusaha menjaga stabilitas institusional ketika atribusi tanggung jawab belum sepenuhnya terbentuk. Penelitian ini menggunakan istilah stabilisasi institusional dalam kondisi ketidakpastian atribusi untuk membaca pola tersebut, yakni kecenderungan organisasi menjaga kontinuitas layanan, mengurangi ketidakpastian, memberikan langkah perlindungan awal, serta mempertahankan legitimasi kelembagaan sementara status teknis krisis masih dalam proses verifikasi. Istilah ini digunakan sebagai temuan analitis berbasis kasus, bukan sebagai klaim pembentukan teori baru.

Dengan demikian, kebaruan penelitian

ini tidak hanya terletak pada kasus dugaan kebocoran data ASN di BKN atau penggunaan dua teori komunikasi krisis secara bersamaan. Kontribusi utamanya terletak pada upaya menjelaskan hubungan antara diagnosis atribusi krisis dan pengelolaan reputasi pada kondisi ketika penyebab dan tanggung jawab atas insiden belum terkonfirmasi secara final. Pendekatan tersebut memungkinkan penelitian untuk membedakan antara upaya stabilisasi operasional dan kebutuhan pemulihan reputasional. Penegasan bahwa layanan tetap berjalan, misalnya, dapat berfungsi mengurangi ketidakpastian mengenai kontinuitas pelayanan, tetapi tidak otomatis menjawab kebutuhan informasi mengenai risiko yang mungkin dihadapi oleh subjek data. Perbedaan fungsi komunikasi tersebut menjadi penting dalam memahami bagaimana krisis siber pada lembaga pemerintah perlu dikelola.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan menganalisis strategi komunikasi krisis BKN dalam merespons dugaan kebocoran data ASN tahun 2024 melalui integrasi SCCT dan Image Repair Theory. Secara khusus, penelitian diarahkan untuk mengidentifikasi bagaimana BKN mengonstruksi posisi dan atribusi tanggung jawab terhadap krisis, bagaimana strategi respons digunakan pada fase awal insiden, serta bagaimana pesan-pesan tersebut berfungsi dalam pengelolaan reputasi institusional. Penelitian ini diharapkan memberikan kontribusi teoretis dengan

memperlihatkan fungsi komplementer SCCT sebagai kerangka diagnosis atribusi krisis dan IRT sebagai kerangka analisis pengelolaan citra. Secara praktis, penelitian diharapkan memberikan pemahaman mengenai pentingnya komunikasi krisis yang tidak hanya mempertahankan kontinuitas pelayanan, tetapi juga memberikan informasi yang relevan bagi pemangku kepentingan dalam menghadapi ketidakpastian dan risiko kebocoran data pada lembaga pemerintah.

TINJAUAN PUSTAKA

Kebocoran Data sebagai Krisis Reputasi

Kebocoran data dalam lingkungan digital tidak hanya menimbulkan persoalan teknis mengenai keamanan sistem, tetapi juga dapat berkembang menjadi krisis organisasi karena mengancam kepercayaan dan reputasi institusi. Kondisi tersebut menjadi semakin penting ketika insiden melibatkan lembaga pemerintah yang mengelola data publik dalam jumlah besar. Data yang dikelola oleh institusi pemerintah tidak hanya memiliki fungsi administratif, tetapi juga berkaitan dengan hak subjek data, legitimasi tata kelola, serta kemampuan negara dalam memberikan perlindungan terhadap informasi yang berada di bawah pengelolaannya. Oleh karena itu, ketika terjadi dugaan kebocoran data, penilaian terhadap organisasi tidak hanya berhubungan dengan penyebab teknis insiden, tetapi juga dengan cara organisasi menjelaskan situasi dan merespons kekhawatiran pemangku kepentingan.

Arquelau et al. (2023) menunjukkan bahwa kebocoran data merupakan persoalan multidimensional yang berkaitan dengan keamanan informasi sekaligus kerangka perlindungan data. Dalam konteks organisasi, dampak kebocoran tidak berhenti pada hilangnya atau tersebarnya informasi, tetapi dapat berkembang menjadi ancaman terhadap kredibilitas institusi. Hal tersebut terjadi karena sebagian besar pemangku kepentingan tidak memiliki akses langsung terhadap proses investigasi teknis. Akibatnya, penilaian terhadap kemampuan organisasi dalam menangani insiden juga dipengaruhi oleh informasi yang tersedia dan bagaimana informasi tersebut dikomunikasikan.

Dalam perspektif komunikasi krisis, situasi tersebut menempatkan komunikasi sebagai bagian integral dari penanganan insiden. Coombs (2007) menjelaskan bahwa komunikasi krisis merupakan bagian dari upaya organisasi dalam menyediakan informasi kepada pemangku kepentingan sekaligus mengelola ancaman terhadap reputasi. Dengan demikian, keberhasilan penanganan krisis tidak hanya ditentukan oleh kemampuan organisasi mengatasi sumber gangguan, tetapi juga oleh kemampuan memberikan informasi yang membantu pemangku kepentingan memahami situasi, melindungi diri, dan menilai tindakan yang dilakukan organisasi.

Karakter kebocoran data juga berbeda dari sejumlah krisis organisasi lainnya karena status peristiwa, sumber insiden, dan tingkat

tanggung jawab organisasi tidak selalu dapat diketahui secara langsung pada fase awal. Proses investigasi keamanan siber membutuhkan waktu, sementara informasi mengenai dugaan kebocoran dapat menyebar dengan cepat melalui media dan ruang digital. Kondisi tersebut dapat menghasilkan ketidakpastian mengenai siapa yang bertanggung jawab, seberapa besar dampak yang terjadi, dan apakah organisasi telah melakukan perlindungan yang memadai. Dalam situasi tersebut, komunikasi organisasi berhadapan dengan dua kebutuhan yang berjalan secara bersamaan, yaitu memberikan informasi yang cukup kepada pemangku kepentingan dan menghindari klaim yang belum didukung oleh hasil investigasi.

Penelitian terdahulu memperlihatkan bahwa dimensi reputasi dan kepercayaan menjadi bagian penting dari krisis kebocoran data. Diers-Lawson et al. (2021) menunjukkan bahwa pengelolaan hubungan dengan pemangku kepentingan dan komunikasi strategis berperan dalam membangun kapasitas organisasi menghadapi kebocoran data. Chen et al. (2022) menunjukkan bahwa pemulihan kepercayaan setelah insiden keamanan memerlukan respons organisasi yang mampu menjawab ancaman terhadap hubungan dengan pengguna. Sementara itu, Choi et al. (2025) menempatkan pemulihan kepercayaan publik sebagai bagian penting dalam respons reputasional organisasi setelah krisis kebocoran data pada berbagai

jenis organisasi, termasuk lembaga pemerintah. Temuan tersebut memperkuat argumentasi bahwa kebocoran data perlu dipahami sebagai krisis reputasi, bukan semata-mata sebagai gangguan keamanan teknologi.

Dalam konteks BKN, dimensi tersebut menjadi relevan karena data ASN merupakan bagian dari infrastruktur administrasi pemerintahan. Dugaan kebocoran data tidak hanya dapat memunculkan pertanyaan mengenai keamanan sistem, tetapi juga mengenai kemampuan institusi dalam menjaga data yang dipercayakan kepadanya. Oleh karena itu, respons komunikasi BKN perlu dibaca dalam kaitannya dengan upaya mengelola risiko, atribusi tanggung jawab, dan reputasi institusional.

Situational Crisis Communication Theory

Situational Crisis Communication Theory (SCCT) yang dikembangkan oleh Coombs menjelaskan bahwa strategi respons organisasi dalam krisis perlu mempertimbangkan bagaimana pemangku kepentingan mengatribusikan tanggung jawab terhadap organisasi. Prinsip utama SCCT adalah bahwa tingkat ancaman reputasi tidak hanya ditentukan oleh karakter peristiwa, tetapi juga oleh sejauh mana organisasi dipandang bertanggung jawab atas terjadinya krisis. Semakin besar tanggung jawab yang dilekatkan kepada organisasi, semakin tinggi pula potensi kerusakan reputasi dan semakin besar kebutuhan terhadap respons yang menunjukkan

penerimaan tanggung jawab serta tindakan perbaikan (Coombs, 2007).

SCCT mengelompokkan krisis ke dalam tiga klaster utama, yaitu *victim crisis*, *accidental crisis*, dan *preventable crisis*. Dalam *victim crisis*, organisasi dipersepsikan memiliki tanggung jawab yang rendah karena organisasi juga menjadi korban dari peristiwa yang berasal dari faktor eksternal, seperti bencana, sabotase, atau serangan dari pihak luar. Pada *accidental crisis*, tanggung jawab organisasi berada pada tingkat moderat karena krisis muncul dari kejadian yang tidak disengaja. Adapun pada *preventable crisis*, organisasi dipersepsikan memiliki tingkat tanggung jawab yang tinggi karena krisis diasosiasikan dengan kelalaian, pelanggaran, atau tindakan yang seharusnya dapat dihindari.

Klasifikasi tersebut penting dalam konteks kebocoran data karena posisi organisasi tidak selalu dapat ditentukan secara sederhana. Apabila insiden terjadi karena serangan eksternal, organisasi dapat mengonstruksi dirinya sebagai korban. Namun, sebagai pengelola data, organisasi tetap dapat menghadapi atribusi tanggung jawab apabila pemangku kepentingan menilai bahwa sistem keamanan, prosedur perlindungan, atau tata kelola data seharusnya mampu mencegah atau meminimalkan insiden. Dengan demikian, krisis kebocoran data dapat menghadirkan kondisi atribusional yang tidak stabil, terutama ketika penyebab teknis belum

terverifikasi.

Selain klasifikasi krisis, SCCT juga membedakan sejumlah strategi respons. *Instructing information* merujuk pada informasi yang diberikan untuk membantu pemangku kepentingan melindungi diri dari dampak krisis. Dalam krisis kebocoran data, bentuknya dapat berupa panduan pengamanan akun, perubahan kata sandi, atau langkah mitigasi lainnya. *Adjusting information* berfungsi membantu pemangku kepentingan memahami situasi dan mengurangi ketidakpastian maupun kecemasan. Sementara itu, *diminish* digunakan untuk mengurangi persepsi mengenai tingkat tanggung jawab organisasi atau tingkat keparahan krisis. Adapun *bolstering* diarahkan pada penguatan persepsi positif terhadap organisasi melalui penekanan terhadap komitmen, kompetensi, rekam jejak, atau tindakan yang mendukung legitimasi institusi (Coombs, 2007).

Dalam penelitian ini, SCCT digunakan terutama untuk menganalisis dimensi atribusional dalam komunikasi BKN. Analisis diarahkan pada bagaimana status krisis dikonstruksi, sejauh mana tanggung jawab institusional ditempatkan dalam pesan, serta strategi respons yang digunakan ketika penyebab dan status dugaan kebocoran belum terkonfirmasi secara final. Dengan posisi tersebut, SCCT tidak digunakan hanya untuk memberikan label terhadap pesan, tetapi sebagai kerangka untuk memahami hubungan antara konstruksi krisis, atribusi

tanggung jawab, dan pilihan respons organisasi.

Image Repair Theory

Image Repair Theory (IRT) yang dikembangkan Benoit berangkat dari asumsi bahwa citra dan reputasi merupakan aset penting bagi organisasi. Ketika organisasi dikaitkan dengan tindakan atau peristiwa yang dianggap merugikan, organisasi akan berupaya membangun pesan yang dapat mengurangi ancaman terhadap citranya. Fokus utama IRT berada pada strategi diskursif yang digunakan organisasi dalam mempertahankan atau memperbaiki citra ketika menghadapi tuduhan, kritik, atau krisis reputasi (Benoit, 1997).

Benoit mengelompokkan strategi perbaikan citra ke dalam lima kategori utama, yaitu *denial*, *evasion of responsibility*, *reducing offensiveness*, *corrective action*, dan *mortification*. *Denial* digunakan ketika organisasi menyangkal terjadinya suatu tindakan atau menolak keterlibatan dalam peristiwa yang dituduhkan. *Evasion of responsibility* digunakan ketika organisasi mengakui adanya hubungan dengan peristiwa, tetapi berupaya mengurangi tingkat tanggung jawab dengan menunjukkan bahwa tindakan terjadi karena faktor tertentu, keterbatasan kontrol, atau ketidaksengajaan. *Reducing offensiveness* bertujuan mengurangi persepsi negatif terhadap peristiwa dengan menurunkan tingkat keburukan atau menonjolkan aspek lain yang dinilai positif. *Corrective action* menekankan tindakan

organisasi untuk memperbaiki kondisi dan mencegah terulangnya masalah. Sementara itu, *mortification* dilakukan melalui pengakuan terhadap kesalahan dan penyampaian permintaan maaf.

IRT relevan dalam krisis kebocoran data karena komunikasi organisasi pada situasi tersebut tidak hanya berfungsi menyampaikan informasi, tetapi juga membawa konsekuensi reputasional. Penekanan terhadap keberlanjutan pelayanan, pelaksanaan investigasi, koordinasi dengan otoritas lain, atau tindakan mitigasi dapat berfungsi sekaligus sebagai informasi publik dan sebagai strategi untuk menunjukkan kompetensi serta tanggung jawab institusi.

Namun, penggunaan kategori IRT perlu memperhatikan konteks dan bukti tekstual secara hati-hati. Tidak setiap bentuk kehati-hatian bahasa dapat langsung diposisikan sebagai strategi penghindaran tanggung jawab. Misalnya, penggunaan istilah “dugaan” dalam konteks investigasi yang belum selesai dapat menunjukkan kehati-hatian institusional sebelum memperoleh kepastian teknis. Oleh karena itu, kategori *evasion of responsibility* perlu didasarkan pada pesan yang secara lebih eksplisit menunjukkan upaya membatasi, mengurangi, atau mengalihkan tanggung jawab, bukan semata-mata pada penggunaan istilah yang mencerminkan status investigasi.

Dalam penelitian ini, IRT digunakan untuk membaca fungsi reputasional pesan yang disampaikan oleh BKN. Analisis tidak

diarahkan untuk menentukan benar atau salahnya institusi secara teknis, tetapi untuk memahami bagaimana konstruksi pesan digunakan dalam merespons ancaman terhadap citra. Dengan demikian, IRT melengkapi analisis SCCT dengan memberikan perhatian yang lebih rinci terhadap bagaimana organisasi mempertahankan legitimasi melalui pilihan pesan yang digunakan selama krisis.

Integrasi SCCT dan IRT

SCCT dan IRT sama-sama menempatkan reputasi sebagai elemen penting dalam komunikasi krisis, tetapi keduanya memiliki titik tekan analitis yang berbeda. SCCT berfokus pada hubungan antara karakter krisis, atribusi tanggung jawab, tingkat ancaman reputasi, dan pemilihan strategi respons. Sementara itu, IRT lebih menekankan bentuk-bentuk wacana yang digunakan organisasi ketika citranya menghadapi ancaman. Perbedaan tersebut memungkinkan kedua teori digunakan secara komplementer, sepanjang integrasinya tidak berhenti pada penggabungan dua daftar kategori.

Dalam penelitian ini, SCCT ditempatkan sebagai kerangka diagnosis atribusi krisis, sedangkan IRT berfungsi sebagai kerangka interpretasi pengelolaan reputasi. Tahap diagnosis melalui SCCT digunakan untuk melihat bagaimana BKN memosisikan status krisis, bagaimana tanggung jawab dibingkai, serta strategi respons apa yang digunakan. Selanjutnya, IRT digunakan untuk menelaah fungsi reputasional dari pilihan pesan

tersebut, seperti apakah pesan berfungsi mengurangi tingkat ofensivitas krisis, menunjukkan langkah korektif, mengakui kesalahan, atau membatasi tanggung jawab.

SCCT terutama membantu menjelaskan dua tahap pertama dan hubungan keduanya dengan pilihan respons, sedangkan IRT memperdalam analisis pada fungsi reputasional dari pesan yang digunakan organisasi. Melalui hubungan ini, satu pesan dapat memiliki lebih dari satu fungsi analitis. Sebagai contoh, pernyataan mengenai keberlanjutan layanan dapat dibaca sebagai *adjusting information* apabila berfungsi mengurangi ketidakpastian pemangku kepentingan, tetapi pada saat yang sama dapat memiliki fungsi *reducing offensiveness* apabila pesan tersebut menurunkan persepsi terhadap luasnya dampak krisis. Dengan demikian, tumpang tindih antarkategori tidak diperlakukan sebagai kelemahan, melainkan sebagai indikasi bahwa satu pesan dapat bekerja secara simultan pada dimensi perlindungan pemangku kepentingan dan pengelolaan reputasi.

Integrasi tersebut juga memungkinkan penelitian membedakan antara stabilisasi operasional dan pengelolaan reputasional. Stabilisasi operasional berkaitan dengan upaya meyakinkan pemangku kepentingan bahwa fungsi institusi dan pelayanan tetap berlangsung, sedangkan pengelolaan reputasional berkaitan dengan bagaimana organisasi menjaga kepercayaan, legitimasi, dan persepsi mengenai tanggung jawab

institusional. Dalam krisis kebocoran data, kedua dimensi tersebut dapat berlangsung bersamaan tetapi tidak selalu menghasilkan efek yang sama. Pernyataan bahwa layanan tetap berjalan, misalnya, dapat menjawab kekhawatiran mengenai kontinuitas administrasi, tetapi belum tentu menjawab ketidakpastian mengenai data apa yang terdampak dan risiko apa yang dihadapi oleh subjek data.

Oleh karena itu, penggunaan SCCT dan IRT dalam penelitian ini dimaksudkan untuk menghasilkan pembacaan yang lebih menyeluruh terhadap komunikasi krisis BKN. Analisis tidak hanya ditujukan untuk mengidentifikasi kategori strategi komunikasi, tetapi juga untuk memahami bagaimana strategi tersebut membentuk pola respons institusional ketika status krisis dan atribusi tanggung jawab masih berada dalam proses verifikasi. Kerangka integratif ini menjadi dasar bagi analisis terhadap hubungan antara ketidakpastian atribusi, upaya stabilisasi situasi, dan pengelolaan reputasi dalam konteks krisis siber pada lembaga pemerintah.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus untuk menganalisis strategi komunikasi krisis Badan Kepegawaian Negara (BKN) dalam merespons dugaan kebocoran data Aparatur Sipil Negara (ASN) tahun 2024. Pendekatan kualitatif dipilih karena penelitian berfokus pada penafsiran terhadap konstruksi pesan, atribusi tanggung

jawab, dan fungsi reputasional komunikasi institusional dalam situasi krisis. Desain studi kasus digunakan karena penelitian diarahkan pada satu peristiwa kontemporer yang spesifik dan dianalisis dalam konteksnya secara mendalam (Yin, 2018).

Objek penelitian adalah komunikasi krisis BKN terkait dugaan kebocoran data ASN tahun 2024. Unit analisis berupa pernyataan atau unit pesan yang memuat konstruksi status krisis, atribusi tanggung jawab, informasi perlindungan kepada pemangku kepentingan, keberlanjutan layanan, koordinasi kelembagaan, serta tindakan penanganan krisis. Korpus penelitian terdiri atas empat dokumen yang diterbitkan pada 11 Agustus 2024, yaitu satu Siaran Pers BKN Nomor 007/RILIS/BKN/VIII/2024, satu pemberitaan Antara, satu pemberitaan Kompas, dan satu pemberitaan Tempo. Keempat dokumen tersebut secara langsung membahas dugaan kebocoran data ASN dan respons BKN. Periode tersebut diposisikan sebagai fase awal krisis karena merepresentasikan tahap awal pemberitaan kasus dan munculnya respons resmi pertama BKN.

Pemilihan dokumen didasarkan pada beberapa kriteria inklusi, yaitu: (1) secara langsung membahas dugaan kebocoran data ASN yang dikaitkan dengan BKN; (2) diterbitkan pada fase awal perkembangan kasus; (3) memuat informasi mengenai respons, tindakan, atau posisi BKN terhadap insiden; dan (4) berasal dari sumber yang dapat diverifikasi. Adapun dokumen yang

hanya menyebut kasus secara sepintas, mengulang informasi tanpa memberikan substansi yang relevan, atau tidak memuat informasi mengenai respons BKN tidak dimasukkan dalam korpus penelitian.

Siaran pers BKN digunakan sebagai sumber utama untuk mengidentifikasi konstruksi dan posisi resmi institusi. Sementara itu, pemberitaan Antara, Kompas, dan Tempo digunakan untuk melihat bagaimana kasus dan respons BKN direpresentasikan dalam pemberitaan media pada fase awal krisis. Pemberitaan media dalam penelitian ini tidak diposisikan sebagai representasi langsung persepsi publik, melainkan sebagai representasi atau konstruksi media terhadap peristiwa. Oleh karena itu, penelitian ini tidak menarik kesimpulan mengenai sikap atau persepsi publik secara langsung berdasarkan isi pemberitaan media.

Pengumpulan data dilakukan melalui studi dokumen dan penelusuran arsip digital. Keempat dokumen diorganisasi secara kronologis untuk membaca perkembangan awal isu, respons institusional, dan konstruksi mengenai dampak krisis. Selanjutnya, setiap dokumen dibaca secara berulang untuk mengidentifikasi pernyataan yang relevan dengan pertanyaan penelitian.

Analisis data menggunakan analisis isi kualitatif yang dilakukan melalui tahapan reduksi data, identifikasi unit pesan, pengodean, pengelompokan berdasarkan kategori teoretis, dan interpretasi

(Krippendorff, 2019). Pada tahap pertama, peneliti mengidentifikasi unit pesan yang berkaitan dengan status insiden, atribusi tanggung jawab, instruksi kepada pengguna, keberlanjutan layanan, koordinasi antarlembaga, pengurangan tingkat keparahan krisis, dan tindakan perbaikan. Unit pesan tersebut selanjutnya diberi kode berdasarkan kategori yang diturunkan dari Situational Crisis Communication Theory (SCCT) dan Image Repair Theory (IRT).

Dalam kerangka SCCT, proses pengodean mencakup dua dimensi. Pertama, dimensi atribusi krisis yang meliputi *victim crisis*, *accidental crisis*, dan *preventable crisis*. Kedua, dimensi strategi respons yang meliputi *instructing information*, *adjusting information*, *diminish*, dan *bolstering* (Coombs, 2007). *Instructing information* digunakan untuk mengode pesan yang berisi instruksi perlindungan kepada pengguna; *adjusting information* untuk pesan yang memberikan penjelasan mengenai situasi dan membantu mengurangi ketidakpastian; *diminish* untuk pesan yang membatasi persepsi mengenai tingkat keparahan atau tanggung jawab; dan *bolstering* untuk pesan yang menonjolkan kompetensi, komitmen, atau tindakan positif institusi.

Dalam kerangka IRT, pengodean diarahkan pada kategori *denial*, *evasion of responsibility*, *reducing offensiveness*, *corrective action*, dan *mortification* (Benoit, 1997). *Denial* digunakan apabila terdapat penyangkalan eksplisit terhadap tuduhan atau

keterlibatan organisasi; *evasion of responsibility* digunakan apabila pesan secara eksplisit membatasi atau mengurangi tanggung jawab organisasi; *reducing offensiveness* digunakan ketika pesan berupaya mengurangi persepsi negatif terhadap dampak peristiwa; *corrective action* digunakan untuk tindakan investigasi, mitigasi, atau pencegahan; sedangkan *mortification* digunakan apabila terdapat pengakuan kesalahan atau permintaan maaf secara eksplisit.

Dalam proses pengodean, satu unit pesan dapat memperoleh lebih dari satu kode apabila memiliki fungsi komunikasi yang berbeda. Namun, pemberian kode dilakukan berdasarkan indikator tekstual yang eksplisit. Sebagai contoh, penggunaan istilah “dugaan” tidak secara otomatis dikategorikan sebagai *evasion of responsibility*, karena istilah tersebut dapat pula merepresentasikan kehati-hatian institusional ketika proses investigasi belum selesai. Kategori *evasion of responsibility* hanya digunakan apabila ditemukan pernyataan yang secara eksplisit membatasi, mengurangi, atau mengalihkan tanggung jawab institusi.

Tahap berikutnya adalah interpretasi dengan menghubungkan hasil pengodean dari kedua teori. SCCT digunakan untuk menjelaskan bagaimana status krisis dan atribusi tanggung jawab dikonstruksi serta bagaimana strategi respons dipilih, sedangkan IRT digunakan untuk membaca fungsi reputasional dari pesan tersebut. Dengan

prosedur ini, analisis bergerak dari unit pesan, kode analitis, kategori teoretis, hingga interpretasi, sehingga penelitian tidak hanya memetakan strategi komunikasi, tetapi juga menjelaskan hubungan antara ketidakpastian atribusi dan pengelolaan reputasi institusional.

Untuk menjaga keabsahan analisis, penelitian menggunakan triangulasi sumber dan triangulasi teori. Triangulasi sumber dilakukan dengan membandingkan isi siaran pers resmi BKN dengan representasi kasus dalam pemberitaan Antara, Kompas, dan Tempo. Triangulasi teori dilakukan dengan menggunakan SCCT dan IRT secara komplementer. SCCT digunakan untuk membaca dimensi atribusi dan strategi respons, sedangkan IRT digunakan untuk menginterpretasikan fungsi reputasional dari pesan organisasi.

HASIL DAN PEMBAHASAN

Konstruksi Kronologi Awal Dugaan Kebocoran Data ASN Tahun 2024

Dugaan kebocoran data Aparatur Sipil Negara (ASN) mulai memperoleh perhatian pada Agustus 2024 setelah muncul informasi mengenai penjualan data yang dikaitkan dengan Badan Kepegawaian Negara (BKN) di forum peretas BreachForums. Berdasarkan pemberitaan Antara, akun anonim bernama TopiAx mengklaim memiliki 4.759.218 baris data yang berkaitan dengan ASN. Data yang diklaim tersedia mencakup sejumlah informasi personal dan administratif, seperti nama, tempat dan tanggal lahir, Nomor Induk Pegawai (NIP), nomor Surat Keputusan CPNS dan PNS, golongan, jabatan, instansi, alamat,

nomor identitas, nomor telepon, surat elektronik, serta informasi pendidikan. Data tersebut disebut ditawarkan dengan harga 10.000 dolar Amerika Serikat atau sekitar Rp160 juta (Antara, 2024).

Pemberitaan Kompas dan Tempo juga menempatkan kasus tersebut sebagai dugaan kebocoran data dalam skala besar yang dikaitkan dengan BKN. Ketiga media menonjolkan klaim mengenai jumlah data, jenis data yang diduga terpapar, penjualan data melalui forum peretas, serta kemungkinan konsekuensi terhadap keamanan informasi ASN. Dalam penelitian ini, pemberitaan tersebut diposisikan sebagai konstruksi media atas krisis, bukan sebagai representasi langsung dari persepsi publik.

BKN memberikan respons resmi melalui Siaran Pers Nomor 007/RILIS/BKN/VIII/2024 pada 11 Agustus 2024. Dalam siaran pers tersebut, BKN menyatakan sedang bekerja sama dengan BSSN serta Kementerian Kominfo untuk melakukan identifikasi dan investigasi terhadap isu dugaan kebocoran data ASN. BKN juga menyatakan bahwa dugaan gangguan tersebut tidak berdampak pada layanan manajemen ASN serta mengimbau pengguna layanan untuk melakukan pembaruan kata sandi secara berkala (BKN, 2024).

Berdasarkan keempat dokumen yang dianalisis, terdapat tiga orientasi pesan utama dalam respons awal BKN. Pertama, BKN menempatkan status insiden sebagai dugaan yang masih dalam proses verifikasi dan

investigasi. Kedua, BKN menekankan keberlanjutan layanan manajemen ASN. Ketiga, BKN memberikan instruksi protektif kepada pengguna melalui imbauan untuk memperbarui kata sandi. Selain itu, penyebutan koordinasi dengan BSSN dan Kementerian Kominfo menunjukkan upaya institusi menegaskan bahwa proses penanganan dilakukan bersama otoritas yang relevan.

Konstruksi Atribusi Krisis

Dalam perspektif SCCT, salah satu aspek utama yang dianalisis adalah bagaimana tanggung jawab terhadap krisis dikonstruksi. Hasil analisis menunjukkan bahwa BKN tidak secara eksplisit mengafirmasi bahwa kebocoran data telah terjadi, tetapi juga tidak menyangkal adanya isu yang harus ditangani. Hal tersebut terlihat dari penggunaan istilah “dugaan kebocoran data ASN” serta pernyataan bahwa proses identifikasi dan investigasi masih berlangsung.

Penggunaan istilah tersebut menunjukkan bahwa posisi institusional BKN pada fase awal krisis masih bersifat sementara. Oleh karena itu, data penelitian belum memberikan dasar yang memadai untuk menempatkan kasus secara definitif ke dalam salah satu klaster SCCT. Jika insiden terbukti berasal dari serangan eksternal, kasus dapat mendekati karakteristik *victim crisis* karena organisasi menjadi sasaran tindakan pihak luar. Namun, posisi BKN sebagai pengelola data ASN membuka kemungkinan atribusi tanggung jawab yang lebih besar

apabila kelemahan dalam keamanan atau tata kelola data dipandang memiliki kontribusi terhadap insiden.

Dengan demikian, temuan penelitian lebih tepat menunjukkan adanya ketidakpastian atribusi daripada penempatan kasus secara final sebagai *victim*, *accidental*, atau *preventable crisis*. Ketidakpastian tersebut muncul karena pada fase awal krisis belum tersedia kepastian teknis mengenai sumber, mekanisme, maupun tingkat tanggung jawab organisasi, sedangkan BKN tetap memiliki kewajiban institusional sebagai pengelola data ASN.

Konstruksi tersebut berbeda dengan penekanan pemberitaan media. Antara, Kompas, dan Tempo lebih menonjolkan besarnya jumlah data yang diklaim bocor, jenis data yang diduga tersedia, serta penjualan data melalui forum peretas. Perbedaan ini menunjukkan bahwa komunikasi resmi BKN dan pemberitaan media memberikan penekanan yang berbeda terhadap krisis. BKN menekankan status investigasi dan keberlanjutan layanan, sedangkan pemberitaan media lebih menonjolkan potensi skala dan tingkat keseriusan insiden.

Strategi Respons BKN Berdasarkan SCCT

Hasil pengodean menunjukkan empat bentuk utama strategi respons yang dapat dibaca melalui SCCT, yaitu *instructing information*, *adjusting information*, *diminish*, dan *bolstering*.

Pertama, *instructing information* terlihat dari imbauan BKN kepada pengguna

layanan untuk memperbarui kata sandi secara berkala. Pesan tersebut merupakan bentuk informasi protektif karena memberikan tindakan yang dapat dilakukan pengguna untuk mengurangi potensi risiko terhadap akun yang mereka gunakan. Dalam korpus penelitian, imbauan perubahan kata sandi merupakan instruksi paling konkret yang diberikan BKN kepada pemangku kepentingan pada fase awal krisis.

Kedua, *adjusting information* terlihat melalui pernyataan bahwa layanan manajemen ASN tetap berjalan dan dugaan gangguan tidak memengaruhi layanan yang digunakan masyarakat. Pesan tersebut menyediakan informasi mengenai kondisi operasional institusi dan berfungsi mengurangi ketidakpastian mengenai kemungkinan terganggunya pelayanan kepegawaian. BKN dengan demikian tidak hanya merespons isu keamanan data, tetapi juga memberikan kepastian mengenai kontinuitas pelayanan.

Ketiga, strategi *diminish* terlihat dari penekanan bahwa dugaan gangguan tidak berdampak terhadap layanan manajemen ASN. Pernyataan tersebut membatasi ruang dampak krisis pada isu keamanan data tanpa mengaitkannya dengan kegagalan fungsi pelayanan secara keseluruhan. Dalam konteks ini, strategi *diminish* tidak berarti BKN menyangkal adanya isu, tetapi mengurangi persepsi mengenai luasnya dampak operasional yang ditimbulkan.

Keempat, *bolstering* muncul melalui

penekanan terhadap koordinasi BKN dengan BSSN dan Kementerian Kominfo. Penyebutan keterlibatan institusi yang memiliki kewenangan dalam keamanan siber dan tata kelola komunikasi digital memperkuat pesan bahwa BKN melakukan penanganan secara terkoordinasi. Pesan tersebut sekaligus menampilkan tindakan organisasi sebagai bagian dari respons kelembagaan yang melibatkan otoritas terkait.

Hasil tersebut menunjukkan bahwa komunikasi awal BKN tidak hanya menggunakan satu jenis strategi, tetapi mengombinasikan pesan protektif, penenangan situasi, pembatasan dampak, dan penguatan legitimasi kelembagaan.

Strategi Pengelolaan Citra Berdasarkan Image Repair Theory

Analisis dengan Image Repair Theory menunjukkan bahwa kategori yang paling kuat didukung oleh data adalah *reducing offensiveness* dan *corrective action*. Strategi *reducing offensiveness* terlihat terutama melalui pernyataan BKN bahwa dugaan gangguan tidak berdampak pada layanan manajemen ASN. Dengan menekankan keberlanjutan fungsi pelayanan, BKN membatasi persepsi terhadap luasnya konsekuensi institusional dari krisis. Pesan tersebut tidak menyangkal isu kebocoran data, tetapi memberikan penekanan pada aspek organisasi yang tetap berjalan normal.

Sementara itu, *corrective action* terlihat melalui proses identifikasi dan investigasi bersama BSSN dan Kementerian Kominfo

serta imbauan kepada pengguna untuk memperbarui kata sandi. Kedua bentuk pesan tersebut menunjukkan tindakan yang diarahkan pada penanganan dan mitigasi risiko. Meskipun korpus penelitian tidak memberikan informasi mengenai hasil akhir investigasi maupun perubahan sistem yang dilakukan setelah fase awal krisis, tindakan investigasi dan pemberian instruksi keamanan dapat dibaca sebagai bentuk tindakan korektif awal.

Penggunaan kata “dugaan” tidak secara otomatis dikategorikan sebagai *evasion of responsibility*. Istilah tersebut dapat mencerminkan kehati-hatian institusional selama proses investigasi belum selesai. Dalam empat dokumen yang dianalisis, tidak ditemukan pernyataan yang cukup eksplisit untuk menunjukkan bahwa BKN secara langsung memindahkan atau mengalihkan tanggung jawab kepada pihak lain. Oleh karena itu, *evasion of responsibility* tidak ditempatkan sebagai temuan utama penelitian.

Strategi denial juga tidak ditemukan secara eksplisit karena BKN tidak menolak adanya isu yang sedang berkembang. Demikian pula, mortification tidak terlihat dalam respons awal karena tidak ditemukan pengakuan kesalahan atau permintaan maaf secara eksplisit. Absennya *mortification* perlu dibaca dalam konteks bahwa pada fase tersebut hasil investigasi mengenai status dan sumber insiden belum tersedia secara final.

Pembahasan

Stabilisasi Institusional dalam Kondisi Ketidakpastian Atribusi

Jika temuan SCCT dan IRT dibaca secara terpadu, respons BKN memperlihatkan pola yang lebih kompleks daripada sekadar penggunaan beberapa kategori strategi komunikasi. Kombinasi *instructing information*, *adjusting information*, *diminish*, *bolstering*, *reducing offensiveness*, dan *corrective action* menunjukkan adanya orientasi pada stabilisasi institusional dalam kondisi ketidakpastian atribusi.

Pola tersebut muncul ketika organisasi menghadapi situasi ketika status teknis insiden dan tingkat tanggung jawab belum diketahui secara final, tetapi institusi tetap harus memberikan respons kepada pemangku kepentingan. Dalam kondisi tersebut, BKN menjalankan beberapa fungsi komunikasi secara simultan. Imbauan pembaruan kata sandi memberikan tindakan protektif kepada pengguna; pernyataan bahwa layanan tetap berjalan mempertahankan kepastian mengenai kontinuitas operasional; koordinasi dengan BSSN dan Kementerian Kominfo memperkuat legitimasi respons kelembagaan; sedangkan investigasi menunjukkan adanya langkah yang diarahkan pada penanganan insiden.

Temuan tersebut memperlihatkan bahwa strategi komunikasi BKN pada fase awal lebih diarahkan pada menstabilkan situasi daripada memberikan penjelasan final mengenai penyebab atau tanggung jawab

krisis. Pilihan tersebut dapat dipahami karena organisasi berkomunikasi ketika hasil investigasi belum tersedia. Namun, pola ini juga menunjukkan bahwa komunikasi krisis siber menghadirkan dilema antara kebutuhan untuk memberikan kepastian kepada pemangku kepentingan dan kebutuhan institusi untuk tidak menyampaikan klaim teknis yang belum dapat diverifikasi.

Konsep ketidakpastian atribusi menjadi penting karena BKN berada dalam dua posisi sekaligus. Di satu sisi, organisasi dapat menjadi korban apabila data diperoleh melalui tindakan serangan eksternal. Di sisi lain, status BKN sebagai pengelola data menciptakan ekspektasi mengenai kewajiban institusi untuk menjaga keamanan informasi. Oleh sebab itu, ancaman reputasional tidak hanya bergantung pada siapa pelaku serangan, tetapi juga pada bagaimana kemampuan institusi dalam mencegah, mendeteksi, menjelaskan, dan menangani insiden dinilai oleh pemangku kepentingan.

Dengan demikian, hasil penelitian ini memperluas penggunaan SCCT dalam konteks krisis siber dengan menunjukkan bahwa fase awal krisis tidak selalu memungkinkan klasifikasi tanggung jawab yang bersifat final. Dalam kasus semacam ini, analisis perlu memperhatikan proses perubahan atribusi dari waktu ke waktu, bukan hanya menentukan tipe krisis berdasarkan kondisi awal.

Stabilisasi Operasional Tidak Identik dengan Pemulihan Reputasional

Temuan lain yang penting adalah adanya perbedaan antara stabilisasi operasional dan pemulihan reputasional. Pernyataan BKN bahwa layanan manajemen ASN tetap berjalan merupakan informasi penting karena memberikan kepastian bahwa pelayanan administratif tidak mengalami gangguan. Dari perspektif SCCT, pesan ini dapat berfungsi sebagai *adjusting information* karena mengurangi ketidakpastian mengenai keberlangsungan pelayanan. Pada saat yang sama, dalam perspektif IRT, pesan tersebut juga memiliki fungsi *reducing offensiveness* karena membatasi persepsi mengenai luasnya dampak krisis.

Namun, keberlangsungan layanan tidak secara otomatis menjawab seluruh kebutuhan informasi yang muncul dalam krisis kebocoran data. Dalam kasus seperti ini, terdapat setidaknya dua jenis ketidakpastian yang berbeda. Pertama adalah ketidakpastian operasional, yaitu apakah layanan organisasi masih dapat digunakan. Kedua adalah ketidakpastian risiko data, yaitu data apa yang mungkin terdampak, siapa yang berisiko, bagaimana data dapat disalahgunakan, dan tindakan apa yang perlu dilakukan oleh subjek data.

Korpus penelitian menunjukkan bahwa respons awal BKN lebih jelas menjawab jenis ketidakpastian pertama. BKN menegaskan bahwa layanan tetap berjalan dan memberikan instruksi untuk memperbarui kata sandi. Namun, empat dokumen yang dianalisis belum menunjukkan adanya

penjelasan terperinci mengenai kelompok data yang berpotensi terdampak, tingkat risiko bagi pemilik data, mekanisme notifikasi individual, atau jadwal pembaruan informasi mengenai hasil investigasi.

Temuan ini penting karena memperlihatkan bahwa kontinuitas pelayanan dan keamanan data merupakan dua dimensi komunikasi yang berbeda. Organisasi dapat berhasil mempertahankan stabilitas pelayanan tanpa sepenuhnya menyelesaikan ketidakpastian reputasional yang berkaitan dengan keamanan dan perlindungan data pribadi.

Hal tersebut sejalan dengan pandangan bahwa krisis kebocoran data tidak berhenti pada gangguan sistem, tetapi berkaitan dengan hubungan dan kepercayaan antara organisasi dengan pemangku kepentingannya. Diers-Lawson et al. (2021) menekankan pentingnya hubungan pemangku kepentingan dan komunikasi strategis dalam membangun kapasitas menghadapi *data breach*. Chen et al. (2022) juga menunjukkan bahwa pemulihan kepercayaan setelah insiden keamanan tidak hanya terkait dengan pemulihan fungsi sistem, tetapi dengan cara organisasi menangani hubungan dengan pengguna. Dalam konteks ini, respons BKN memperlihatkan bahwa fungsi operasional dan fungsi reputasional komunikasi perlu dipahami secara terpisah sekaligus saling terkait.

Integrasi SCCT dan Image Repair Theory

Integrasi SCCT dan IRT menghasilkan pembacaan yang lebih luas dibanding

penggunaan salah satu teori secara terpisah. SCCT menjelaskan bagaimana krisis dan tanggung jawab diposisikan, sedangkan IRT membantu menjelaskan fungsi reputasional dari pilihan pesan organisasi.

Misalnya, pernyataan bahwa layanan manajemen ASN tetap berjalan dapat dikategorikan sebagai *adjusting information* ketika dilihat dari fungsinya dalam memberikan kepastian kepada pemangku kepentingan. Namun, pesan yang sama juga dapat dipahami sebagai *reducing offensiveness* karena mengurangi persepsi bahwa krisis telah mengganggu seluruh fungsi institusi. Demikian pula, koordinasi dengan BSSN dan Kementerian Kominfo dapat dibaca sebagai *bolstering* karena memperkuat legitimasi institusional, sedangkan proses investigasi yang dilakukan bersama dapat dipahami sebagai *corrective action* ketika dilihat sebagai tindakan penanganan krisis.

Tumpang tindih tersebut menunjukkan bahwa SCCT dan IRT tidak perlu diperlakukan sebagai dua sistem klasifikasi yang saling bersaing. Sebaliknya, keduanya dapat digunakan untuk menjelaskan lapisan fungsi komunikasi yang berbeda. SCCT membantu mendiagnosis posisi organisasi terhadap krisis dan strategi respons yang digunakan, sedangkan IRT memperdalam analisis mengenai bagaimana pesan tersebut bekerja dalam mempertahankan atau memperbaiki citra.

Dengan demikian, kontribusi konseptual penelitian ini terletak pada

penggunaan kedua teori untuk menjelaskan alur:

ketidakpastian krisis → atribusi tanggung jawab → pilihan respons → fungsi reputasional pesan. Alur tersebut memungkinkan analisis melampaui pertanyaan mengenai “strategi apa yang digunakan BKN” menuju pertanyaan yang lebih penting, yaitu “bagaimana kombinasi strategi tersebut bekerja ketika tanggung jawab terhadap krisis belum terkonfirmasi secara final”.

Posisi Temuan terhadap Penelitian Terdahulu

Temuan penelitian ini memiliki titik temu sekaligus perbedaan dengan kajian sebelumnya. Penelitian Febriandy dan Wahyutama mengenai krisis PDNS menempatkan Image Repair Theory sebagai kerangka untuk membaca strategi pemerintah dalam menghadapi ancaman reputasi. Penelitian Maulana dan Nasrulloh (2024) juga menunjukkan penggunaan strategi pemulihan citra setelah dugaan serangan siber terhadap Bank Syariah Indonesia. Sementara itu, Tannavaro dan Wiraguna (2025) menegaskan pentingnya fungsi humas dalam pengelolaan krisis siber.

Studi ini memperluas kajian tersebut dengan menempatkan strategi pengelolaan citra dalam kaitannya dengan atribusi tanggung jawab yang belum stabil. Dalam kasus BKN, strategi reputasional tidak berlangsung setelah penyebab krisis diketahui secara pasti, tetapi justru muncul ketika

proses investigasi masih berjalan. Hal ini membuat komunikasi organisasi bukan hanya berfungsi memperbaiki citra setelah krisis, tetapi juga mengelola ekspektasi dan legitimasi selama definisi krisis sendiri masih terbentuk.

Temuan juga memiliki hubungan dengan penelitian Nurhayati dan Laksmi (2023) mengenai *framing* kebocoran data PeduliLindungi. Dalam kasus BKN, pemberitaan media juga menonjolkan elemen yang berbeda dari komunikasi institusional. Ketiga pemberitaan media dalam korpus penelitian memberikan penekanan lebih besar pada jumlah data, jenis data, harga penjualan, dan potensi validitas data, sedangkan BKN menekankan investigasi, kontinuitas layanan, tindakan perlindungan, dan koordinasi kelembagaan. Namun, penelitian ini tidak menyimpulkan bahwa *framing* media tersebut identik dengan persepsi publik. Sebaliknya, perbedaan penekanan tersebut menunjukkan adanya arena komunikasi yang melibatkan lebih dari satu konstruksi mengenai krisis.

Temuan penelitian ini juga relevan dengan Choi et al. (2025), yang menekankan bahwa pemulihan kepercayaan setelah *data breach* berkaitan erat dengan strategi respons reputasional organisasi. Kasus BKN memperlihatkan bahwa proses tersebut dapat dimulai sejak fase awal melalui tindakan korektif dan penegasan koordinasi, tetapi keberlanjutan pemulihan kepercayaan membutuhkan komunikasi yang melampaui penegasan stabilitas pelayanan.

Implikasi Teoretis dan Praktis

Secara teoretis, hasil penelitian memperlihatkan bahwa SCCT dan IRT dapat digunakan secara komplementer untuk membaca krisis siber pemerintah, terutama dalam situasi ketika atribusi tanggung jawab belum bersifat final. SCCT memberi dasar untuk memahami posisi tanggung jawab dan pilihan respons, sedangkan IRT memungkinkan analisis mengenai konsekuensi reputasional dari pesan yang digunakan. Integrasi tersebut menunjukkan bahwa satu pesan dapat sekaligus menjalankan fungsi informasional, atribusional, dan reputasional.

Penelitian juga menunjukkan bahwa dalam krisis siber, klasifikasi tipe krisis perlu diterapkan secara hati-hati. Status organisasi sebagai korban serangan eksternal tidak dengan sendirinya menghilangkan atribusi tanggung jawab yang muncul dari perannya sebagai pengelola data. Dengan demikian, atribusi dalam krisis data lebih tepat dipahami sebagai proses yang dapat berubah mengikuti perkembangan hasil investigasi dan informasi yang tersedia.

Secara praktis, temuan menunjukkan bahwa komunikasi pada fase awal krisis siber perlu mengombinasikan beberapa kebutuhan. Organisasi perlu memberikan instruksi perlindungan yang konkret, menjelaskan kondisi pelayanan, menyampaikan perkembangan proses investigasi, serta memberikan informasi mengenai risiko yang

relevan bagi subjek data. Penekanan pada kontinuitas pelayanan penting untuk mempertahankan stabilitas institusional, tetapi perlu disertai komunikasi risiko agar pemangku kepentingan dapat memahami konsekuensi yang mungkin mereka hadapi.

Dengan demikian, respons awal terhadap krisis kebocoran data tidak cukup dinilai hanya dari seberapa cepat organisasi memberikan pernyataan, tetapi juga dari bagaimana pesan tersebut menjawab ketidakpastian mengenai status insiden, risiko terhadap subjek data, tindakan perlindungan, dan tanggung jawab institusional. Dalam konteks lembaga pemerintah, keempat aspek tersebut berhubungan langsung dengan upaya mempertahankan legitimasi dan kepercayaan terhadap tata kelola data publik.

SIMPULAN

Penelitian ini menemukan bahwa komunikasi krisis BKN pada fase awal dugaan kebocoran data ASN menunjukkan pola stabilisasi institusional di bawah ketidakpastian atribusi. BKN mengombinasikan pemberian instruksi protektif, penegasan keberlanjutan layanan, pembatasan persepsi dampak operasional, serta koordinasi lintas lembaga ketika status teknis dan tanggung jawab atas insiden belum dikonfirmasi secara final. Integrasi SCCT dan IRT menunjukkan bahwa strategi respons krisis tidak hanya berfungsi mengelola atribusi tanggung jawab, tetapi juga secara simultan membentuk upaya perlindungan reputasi institusional.

Secara teoretis, penelitian ini menunjukkan fungsi komplementer kedua kerangka: SCCT membantu menjelaskan diagnosis atribusi dan pemilihan respons, sedangkan IRT membantu menginterpretasikan fungsi reputasional dari konstruksi pesan. Temuan juga memperlihatkan bahwa stabilisasi operasional dan pemulihan kepercayaan merupakan dua kebutuhan komunikasi yang tidak selalu identik. Secara praktis, lembaga pemerintah yang menghadapi krisis data perlu mengombinasikan informasi mengenai kontinuitas layanan dengan informasi yang secara langsung menjawab risiko yang dihadapi subjek data, tindakan perlindungan yang dapat dilakukan, dan perkembangan investigasi.

Penelitian ini memiliki keterbatasan karena menggunakan korpus dokumen pada fase awal krisis dan tidak mengukur respons atau persepsi pemangku kepentingan secara langsung. Pemberitaan media dalam penelitian ini merepresentasikan konstruksi media atas kasus, bukan persepsi publik. Penelitian berikutnya dapat menguji pola yang ditemukan melalui wawancara, analisis respons pengguna media sosial, survei pemangku kepentingan, atau perbandingan beberapa kasus kebocoran data pemerintah.

DAFTAR PUSTAKA

- Antara. (2024). *CISSReC ungkap dugaan kebocoran data BKN*. Antara News. <https://www.antaranews.com/berita/4252647/cissrec-ungkap-dugaan-kebocoran-data-bkn>
- Arquellau, G., Rodrigues, P., Luiz, A., Serrano, M., Nunes, A., Espiñeira, L., ... & Villalba, G. (2023). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. In *International Conference on Data Technologies and Applications* (Vol. 9, No. 27, pp. 1-24).
- Badan Kepegawaian Negara. (2025). *Peraturan Badan Kepegawaian Negara Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Badan Kepegawaian Negara*.
- Badan Kepegawaian Negara. (2022). *Peraturan Badan Kepegawaian Negara Nomor 13 Tahun 2022 tentang Satu Data Bidang Aparatur Sipil Negara*.
- Badan Kepegawaian Negara. (2024). *BKN Pastikan Dugaan Kebocoran Data ASN tidak Mengganggu Layanan Manajemen ASN*. Siaran Pers Nomor: 007/RILIS/BKN/VIII/2024 tanggal 11 Agustus 2024.
- Benoit, W. L. (1997). *Image Repair Discourse and Crisis Communication*. *Public Relations Review*, 23(2), 177–186.
- Chen, A., Wan, J., & Lu, Y. (2022). Repairing the trust in ride-sharing after security incidents. *Industrial Management & Data Systems*, 122(1), 118–136. <https://doi.org/10.1108/IMDS-10-2020-0623>

- Choi, J., Robinson, S., Ruddle, T., & Fister, A. (2025). Restoring Public Trust After a Data Breach Crisis: Reputational Response Strategies for Government, For-Profit, and Nonprofit Organizations. *Risk, Hazards & Crisis in Public Policy*, 16(3).
<https://doi.org/10.1002/rhc3.70026>
- Coombs, W. T. (2007). *Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory*. *Corporate Reputation Review*, 10(3), 163–176.
- DataReportal. (2024). *Digital 2024: Indonesia*.
- Diers-Lawson, A., Symons, A., & Zeng, C. (2021). Building crisis capacity with data breaches: the role of stakeholder relationship management and strategic communication. *Corporate Communications: An International Journal*, 26(4), 675–699.
<https://doi.org/10.1108/CCIJ-02-2021-0024>
- Dirgantoro, Ganet, & Patrianti, Tria. (2025). Strategi Komunikasi Korporat AXA Mandiri Dalam Menjaga Reputasi. *Petanda : Jurnal Ilmu Komunikasi dan Humaniora*. Vol. 07, No. 03 (2025), pp. 367-381.
<https://doi.org/10.32509/petanda.v7i3.5875Ganet>
- Estaswara, H., & Anggraeni, D. (2018). Mengelola *corporate crisis* melalui transformasi model *stakeholder relations* di era digital. *CoverAge: Journal of Strategic Communication*, 9(1), 1–16.
- Febriandy, R. K., & Wahyutama. (2025). Kebocoran Data PDNS Analisis Strategi Komunikasi Krisis Pemerintah Berdasarkan Image Repair Theory. *Communicology: Jurnal Ilmu Komunikasi*, 12(2), 325–341.
<https://doi.org/10.21009/COMM.033.09>
- Kompas. (2024, Agustus 11). *BKN Diduga Diretas, Peretas Tawarkan Data ASN Rp 160 Juta*. Kompas.
<https://www.kompas.id/artikel/bkn-diduga-diretas-peretas-tawarkan-data-asn-rp-160-juta>
- Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology* (4th ed.). SAGE.
- Maulana, B. R., & Nasrulloh. (2024). *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber*. EKSISBANK (Ekonomi Syariah dan Bisnis Perbankan), Volume 8, Nomor 1, Juni 2024.
- Najib, M. (2023). Strategi Komunikasi Krisis BKN terhadap Kecurangan Seleksi Calon Aparatur Sipil Negara Tahun 2021. *Academic Journal of Da'wa and Communication*, 4(01-06), 1–22.
- Nguyen, D., Nguyen, S., Le, P. H., Oomen, T., & Wang, Y. (2024). Utilizing computational methods for analysing media framing of organizational crises: The ‘Datalek’

scandal during the COVID-19 pandemic in the Netherlands.

Journal of Contingencies and Crisis Management, 32(3).

<https://doi.org/10.1111/1468-5973.12595>

Nurhayati, E. S., & Laksmi, L. (2023). Analisis Framing Model Entman pada Pemberitaan Kebocoran Data Aplikasi Pedulilindungi oleh Media Online. *Anuva: Jurnal Kajian Budaya, Perpustakaan, dan Informasi*, 7(4), 573-590.

Panggabean, M.V., & Fitria, A. (2025). Perlindungan Hukun Data Pribadi di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan). *Arus Jurnal Sosial dan Humaniora*, 5 (2), 1958-1965.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran

Negara Republik Indonesia Tahun 2022 Nomor 196.

Safira et al. (2025). Analisis Kepatuhan Etika Profesi Dan Keamanan Sistem: Studi Kasus Kebocoran Data BPJS Kesehatan. *Jurnal Informasi Interaktif* Vol. 10 No. 2 Mei 2025, 2527-5240.

Tannavaro, D.M., & Wiraguna, S.A. (2025). Strategi Komunikasi Humas Dalam Krisis Siber: Studi Kasus BPJS Kesehatan Dan Bank Syariah Indonesia. *Kohesi: Jurnal Multidisiplin Saintek*, Volume 7 No 11 Tahun 2025.

Tempo. (2024, Agustus 11). *Data Pribadi PNS di BKN Diduga Bocor, Dijual Rp 160 juta di BreachForums*. Tempo.
<https://www.tempo.co/ekonomi/data-pribadi-pns-di-bkn-diduga-bocor-dijual-rp-160-juta-di-breachforums-26828>

Yin, R. K. (2018/6th ed. page). *Case Study Research and Applications: Design and Methods*. SAGE.