STRATEGI KOMUNIKASI HUMAS DALAM KRISIS SIBER: STUDI KASUS BPJS KESEHATAN DAN BANK SYARIAH INDONESIA

Devianty Milania Tannavaro[1], Sidi Ahyar Wiraguna[2]
[1]Fakultas Ilmu Komunikasi Universitas Esa Unggul Jakarta
[2]Fakultas Hukum Universitas Esa Unggul Jakarta
Jl. Arjuna Utara Nomor 9, Kebon Jeruk, Jakarta Barat – 11510
[1]milaniaatan@gmail.com, [2]adipatiwiraguna@gmail.com

Abstract

In today's digital era, public trust—or digital trust—has become a crucial asset in fostering long-term relationships between institutions and society. However, this trust can collapse instantly when incidents involving personal data breaches occur within public or private organizations. Major cases such as the BPJS Kesehatan data leak in 2021 and the cyberattack on Bank Syariah Indonesia (BSI) in 2023 highlight the critical importance of data security in institutional communication. During such crises, public relations (PR) professionals play a central role in maintaining the institution's image and restoring public trust. This study aims to explain the strategic role of PR in managing crises resulting from personal data breaches and to identify communication strategies applicable in such situations. The research employs a literature review and case study analysis, drawing on crisis communication theories, PR ethical codes, and relevant regulations such as Law No. 27 of 2022 on Personal Data Protection. The findings indicate that the success of PR in addressing digital trust crises heavily depends on the ability to deliver information promptly, transparently, and ethically, as well as on collaboration with other internal divisions such as IT and legal. With the right approach to communication, PR professionals can assist institutions in recovering their reputation and sustaining public trust amid the challenges of the digital age.
***Keywords**: Public Relations, Digital Trust, Data Breach Crisis, Strategic Communication, Reputation.*

Abstrak

Di era digital saat ini, kepercayaan publik atau digital *trust* menjadi salah satu modal penting dalam membangun hubungan jangka panjang antara institusi dengan masyarakat. Namun, kepercayaan ini bisa runtuh seketika ketika terjadi insiden kebocoran data pribadi yang melibatkan lembaga publik atau swasta. Beberapa kasus besar seperti kebocoran data BPJS Kesehatan pada tahun 2021 dan serangan siber terhadap Bank Syariah Indonesia (BSI) pada tahun 2023 menunjukkan bahwa keamanan data menjadi isu krusial dalam komunikasi lembaga. Ketika krisis ini terjadi, humas sebagai pengelola komunikasi institusi berada di garis depan dalam menjaga stabilitas citra dan membangun kembali kepercayaan publik. Penelitian ini bertujuan untuk menjelaskan peran strategis humas dalam menangani krisis

Article History:
Received: May 2025
Reviewed: May 2025
Published: May 2025

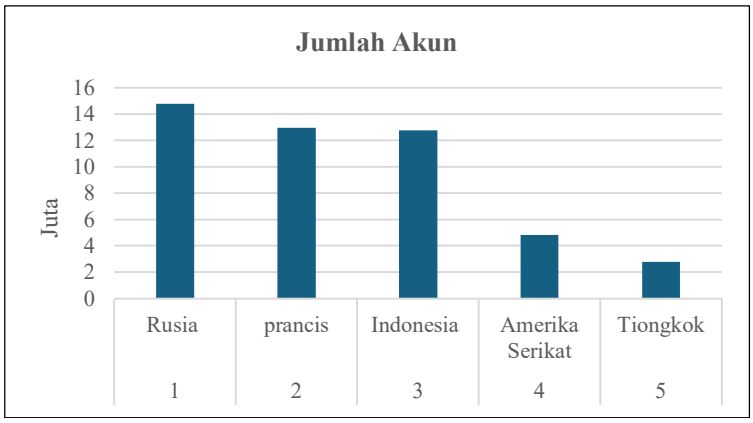
Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

akibat pelanggaran data pribadi, serta mengidentifikasi strategi komunikasi yang dapat diterapkan dalam situasi tersebut. Penelitian dilakukan menggunakan metode studi pustaka dan analisis kasus dengan mengacu pada literatur komunikasi krisis, kode etik humas, serta peraturan perundangan seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Hasil dari penelitian ini menunjukkan bahwa keberhasilan humas dalam menghadapi krisis digital *trust* sangat ditentukan oleh kemampuan dalam menyampaikan informasi secara cepat, terbuka, dan etis, serta kolaborasi dengan divisi internal lainnya seperti IT dan legal. Dengan pendekatan komunikasi yang tepat, humas dapat membantu institusi memulihkan reputasi dan mempertahankan kepercayaan masyarakat di tengah tantangan era digital.
Kata kunci: Humas, Digital *Trust*, Krisis Data, Komunikasi Strategis, Reputasi.

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi telah mengubah berbagai aspek kehidupan manusia, mulai dari cara bekerja, belajar, berkomunikasi, hingga mengakses layanan publik. Dunia kini memasuki era digital, di mana hampir seluruh aktivitas dilakukan secara daring dan berbasis data. Kemajuan ini membawa banyak kemudahan, namun juga menimbulkan tantangan baru, terutama terkait perlindungan privasi dan keamanan informasi pribadi. Era digital telah membawa perubahan besar dalam cara manusia berinteraksi dan mengelola informasi. Transformasi ini juga berdampak pada cara lembaga atau institusi menjalankan operasional dan membangun hubungan dengan masyarakat. Pengumpulan data pribadi menjadi hal yang sangat umum dan bahkan menjadi bagian penting dalam strategi komunikasi, pelayanan, serta pengambilan keputusan yang berbasis data. Namun, di balik kemajuan tersebut, muncul tantangan besar terkait keamanan dan privasi data pribadi yang sering kali belum diantisipasi secara memadai oleh banyak lembaga, baik pemerintah maupun swasta. Salah satu isu yang paling mencolok dalam beberapa tahun terakhir adalah maraknya kebocoran data pribadi di Indonesia. Berdasarkan laporan dari Metro TV News, Indonesia berada di posisi ketiga sebagai negara dengan jumlah kebocoran data terbanyak di dunia.



Sumber: Metro Tv

Isu kebocoran data pribadi menjadi semakin krusial, terutama di era digital ini. Kebocoran data pribadi dapat terjadi melalui berbagai cara, termasuk peretasan, kesalahan manusia, atau kegagalan sistem keamanan. Konsekuensi kebocoran data pribadi dapat sangat merugikan, mulai dari penipuan, penyalahgunaan identitas, hingga kerugian finansial dan reputasi. Kebocoran data pribadi bukan lagi sekadar isu teknis, melainkan juga menjadi krisis kepercayaan (*trust crisis*) yang dapat berdampak langsung pada reputasi institusi. Ketika publik merasa data pribadinya tidak aman, maka kepercayaan terhadap institusi pun berkurang. Hal ini memengaruhi cara pandang masyarakat terhadap kredibilitas dan tanggung jawab lembaga dalam melindungi kepentingan mereka. Salah satu contoh nyata terjadi pada tahun 2021, saat BPJS Kesehatan dikabarkan mengalami kebocoran data yang melibatkan lebih dari 200 juta data penduduk Indonesia dimana data pribadi penduduk termasuk nomor induk kependudukan (NIK), nama, alamat, nomor telepon, bahkan ada yang menyebutkan besaran gaji, diduga bocor dan diperjualbelikan di forum *hacker*. Belum selesai dengan kasus tersebut, pada tahun 2023 Bank Syariah Indonesia (BSI) juga menghadapi krisis diduga akibat serangan siber yang melumpuhkan sistem layanan dan diduga membocorkan data nasabah.

Dalam situasi seperti ini, humas sebagai pengelola komunikasi lembaga memegang peran yang sangat penting. Humas tidak hanya bertanggung jawab untuk menyampaikan informasi kepada publik, tetapi juga bertugas membangun kembali kepercayaan melalui strategi komunikasi yang tepat, responsif, dan etis. Oleh karena itu, penting untuk memahami bagaimana humas seharusnya bertindak dalam situasi krisis yang berkaitan dengan kebocoran data pribadi, serta apa saja tantangan yang dihadapi dalam proses tersebut. Oleh karena itu, penelitian ini bertujuan untuk mengkaji secara mendalam bagaimana peran humas dalam mengelola citra institusi ketika terjadi krisis kebocoran data pribadi, serta mengidentifikasi strategi komunikasi yang digunakan untuk memulihkan kepercayaan publik yang sempat terganggu. Untuk mencapai tujuan tersebut, penelitian ini dilakukan dengan pendekatan kualitatif melalui metode studi pustaka dan analisis kasus, guna memperoleh pemahaman yang komprehensif mengenai dinamika komunikasi krisis, tantangan yang dihadapi praktisi humas, serta praktik terbaik yang dapat dijadikan rujukan dalam menghadapi situasi serupa di masa mendatang.

B. Rumusan Masalah

1. Bagaimana respons komunikasi krisis yang dilakukan oleh BPJS Kesehatan dalam menghadapi kasus kebocoran data tahun 2021 memengaruhi persepsi dan kepercayaan publik?
2. Apa kelemahan strategi komunikasi yang diterapkan oleh Bank Syariah Indonesia dalam menangani serangan siber pada tahun 2023, dan bagaimana dampaknya terhadap citra institusi?
3. Bagaimana perbandingan peran humas dalam strategi komunikasi pada kedua kasus tersebut?
4. Apa tantangan humas dalam mengolah citra institusi di tengah isu serangan siber dan kebocoran data?

TINJAUAN PUSTAKA

A. Humas dan Manajemen Krisis Komunikasi

Humas (Hubungan Masyarakat) merupakan elemen strategis dalam manajemen organisasi yang bertujuan untuk membentuk, memelihara, dan memperbaiki hubungan antara organisasi dan publik internal maupun eksternalnya. Dalam konteks organisasi modern, humas bukan hanya sekadar penyampai informasi, melainkan bertindak sebagai jembatan komunikasi strategis yang menentukan bagaimana citra dan reputasi organisasi dibentuk di mata publik.

Menurut Cutlip, Center, dan Broom (2009), humas adalah “fungsi manajemen yang membangun dan memelihara hubungan timbal balik yang saling menguntungkan antara organisasi dan publiknya melalui komunikasi yang berkelanjutan” (*Effective Public Relations*, 11th *Edition*). Pendekatan ini menekankan pentingnya keterbukaan, kredibilitas, dan konsistensi komunikasi untuk membangun kepercayaan jangka panjang. Dalam situasi krisis, peran humas menjadi semakin krusial. Krisis komunikasi, seperti kebocoran data pribadi, bukan hanya menimbulkan disrupsi operasional tetapi juga dapat menggoyahkan kepercayaan publik secara signifikan.

Oleh karena itu, keberhasilan suatu organisasi dalam mengelola krisis sangat bergantung pada strategi komunikasi yang dijalankan oleh tim humas. Coombs (2007), dalam *Ongoing Crisis Communication*, menyatakan bahwa “komunikasi krisis bukan sekadar tentang memberikan informasi, tetapi juga tentang mengelola persepsi dan emosi publik terhadap organisasi yang sedang mengalami tekanan.” Dalam pandangannya, respons komunikasi yang buruk dapat memperparah krisis, sementara respons yang tepat dan cepat dapat memulihkan atau bahkan meningkatkan reputasi organisasi. Salah satu teori utama dalam manajemen komunikasi krisis adalah *Situational Crisis Communication Theory* (SCCT) yang dikembangkan oleh Timothy Coombs. Teori ini memberikan kerangka kerja sistematis dalam memilih strategi komunikasi berdasarkan dua hal utama: tipe krisis dan tingkat tanggung jawab yang dipersepsikan publik terhadap organisasi. SCCT membagi tipe krisis ke dalam tiga kategori utama:

1. *Victim cluster*, di mana organisasi dianggap sebagai korban (misalnya bencana alam atau rumor tidak benar).
2. *Accidental cluster*, di mana krisis terjadi karena kesalahan tak disengaja.
3. *Preventable cluster*, di mana krisis disebabkan oleh kelalaian atau pelanggaran etika organisasi.

Dalam kasus seperti kebocoran data pribadi, krisis biasanya masuk ke dalam kategori *preventable*, karena publik cenderung menilai bahwa organisasi seharusnya memiliki sistem keamanan yang kuat untuk mencegahnya. Oleh karena itu, strategi komunikasi yang digunakan harus mencerminkan tingkat tanggung jawab tinggi. Coombs menyarankan strategi seperti *apology*, *corrective action*, dan *full disclosure* sebagai bentuk respons yang tepat dalam kategori ini. Studi lain oleh Ulmer, Sellnow, dan Seeger (2010) dalam *Effective Crisis Communication* menekankan pentingnya dialog terbuka, transparansi, dan respons emosional yang empatik dalam membangun kembali kepercayaan setelah krisis. Mereka menekankan bahwa organisasi yang gagal menunjukkan kepedulian terhadap dampak krisis pada publiknya akan menghadapi kesulitan besar dalam memulihkan reputasinya.

Lebih lanjut, Harlow (1976) menggambarkan humas sebagai "fungsi sosial dan manajerial" yang memungkinkan organisasi untuk beradaptasi dengan lingkungan yang berubah dan menghadapi tantangan publik dengan cara yang konstruktif. Dalam hal ini, komunikasi selama krisis harus mempertimbangkan kebutuhan emosional publik, bukan hanya aspek informasi teknis. Oleh karena itu, dalam konteks kebocoran data pribadi, humas tidak hanya harus menyampaikan informasi yang faktual, tetapi juga membangun narasi yang menunjukkan pertanggungjawaban, empati, dan langkah korektif yang jelas. Tanpa pendekatan ini, kepercayaan publik yang telah runtuh akibat pelanggaran privasi akan sulit untuk dipulihkan.

B. Kebocoran Data Pribadi dan Dampaknya terhadap Kepercayaan Publik

Kebocoran data pribadi merupakan ancaman serius di era digital. Ketika data sensitif seperti identitas, kontak, atau informasi keuangan bocor, kepercayaan masyarakat terhadap institusi menjadi terganggu. Menurut Solove (2006), privasi data adalah komponen fundamental dalam menjaga integritas hubungan antara individu dan lembaga. Ketika data pribadi dilanggar, individu merasa rentan, tidak terlindungi, dan cenderung kehilangan kepercayaan terhadap entitas yang mengelola informasi mereka. Hal ini diperkuat oleh Greenleaf (2017) yang menyatakan bahwa ketidakmampuan organisasi dalam melindungi data pribadi dapat merusak hubungan sosial, ekonomi, dan hukum antara organisasi dan pengguna, serta mengganggu keberlangsungan layanan digital yang bergantung pada partisipasi aktif pengguna. Data dari IBM *Security* (2022) menunjukkan bahwa rata-rata biaya kebocoran data secara global mencapai USD 4,35 juta per insiden. Biaya tersebut tidak hanya mencakup pemulihan sistem atau ganti rugi kepada korban, tetapi juga kerugian jangka panjang berupa menurunnya kepercayaan pelanggan, penurunan nilai saham, serta rusaknya reputasi institusi. Dalam jangka panjang, kepercayaan adalah aset yang sulit dipulihkan, dan dalam konteks digital, kepercayaan menjadi salah satu fondasi utama interaksi pengguna.

Di Indonesia, beberapa kasus besar menyoroti lemahnya sistem perlindungan data pribadi. Salah satunya adalah kasus kebocoran data BPJS Kesehatan pada tahun 2021, di mana sekitar 279 juta data penduduk Indonesia, termasuk yang telah meninggal, diklaim bocor dan diperjualbelikan di forum gelap. Data yang bocor mencakup NIK, nama lengkap, tanggal lahir, alamat, dan informasi kependudukan lainnya. Kasus ini mengundang kritik keras dari publik, media, dan pakar keamanan siber, karena institusi pemerintah yang seharusnya menjadi pelindung data justru menjadi titik kebocoran. Kasus lain yang menguatkan kekhawatiran publik adalah serangan siber terhadap Bank Syariah Indonesia (BSI) pada tahun 2023. Serangan ini menyebabkan gangguan layanan selama beberapa hari, dan diduga data nasabah juga ikut diretas dan tersebar di internet. Kedua kasus ini menjadi contoh konkret lemahnya sistem keamanan digital dan manajemen risiko siber di Indonesia. Menurut laporan Metro TV News (2024), Indonesia saat ini menduduki posisi ketiga di dunia sebagai negara dengan jumlah kebocoran data terbanyak, menandakan bahwa digital *trust* masyarakat Indonesia berada dalam situasi yang sangat rentan (Metro TV News, 2024).

Dari perspektif komunikasi, krisis kebocoran data pribadi bukan hanya persoalan teknis, tetapi juga krisis kepercayaan. Seperti dikemukakan oleh Fombrun dan Van Riel (2004), reputasi organisasi sangat bergantung pada persepsi publik mengenai kompetensi, integritas, dan keterbukaan organisasi. Ketika terjadi insiden kebocoran data, ketiga aspek ini langsung dipertanyakan. Jika organisasi gagal memberikan respons komunikasi yang cepat, jujur, dan bertanggung jawab, maka persepsi negatif akan semakin mengakar dan memperburuk kondisi reputasional yang ada. Lebih lanjut, kepercayaan publik (*public trust*) dalam konteks digital atau yang sering disebut digital *trust*, didefinisikan oleh *World Economic Forum* (2020) sebagai keyakinan bahwa teknologi, sistem, dan entitas digital akan bertindak secara bertanggung jawab, aman, dan etis. Dalam hal ini, humas memegang peranan penting dalam menjaga eksistensi digital *trust* dengan menjadi penghubung utama antara institusi dan publik saat terjadi krisis kebocoran data. Dengan demikian, penting bagi lembaga, baik publik maupun swasta, untuk tidak hanya mengandalkan sistem keamanan siber, tetapi juga membangun sistem komunikasi publik yang siap merespons insiden secara strategis. Hal ini sejalan dengan temuan Coombs (2007) dalam teori *Situational Crisis Communication Theory* (SCCT), yang menyatakan bahwa tanggapan organisasi terhadap krisis menentukan besar kecilnya kerusakan reputasi yang ditimbulkan. Tanpa komunikasi yang jelas dan strategis, kepercayaan yang telah dibangun dalam waktu lama dapat runtuh dalam hitungan hari.

C. Digital Trust dan Komunikasi Strategis

Digital *trust* atau kepercayaan digital merujuk pada tingkat keyakinan pengguna bahwa entitas digital—baik berupa lembaga, platform, maupun sistem teknologi—akan melindungi data pribadi mereka, beroperasi secara etis, serta tidak menyalahgunakan informasi yang dikumpulkan. Kepercayaan ini menjadi dasar dalam menjalin interaksi antara masyarakat dan institusi dalam ruang digital. Menurut *World Economic Forum* (2020), digital *trust* merupakan "kemampuan organisasi dan teknologi untuk membangun, mempertahankan, dan mengembangkan kepercayaan melalui prinsip keamanan, transparansi, etika, dan akuntabilitas." Kepercayaan digital bukan hanya berkaitan dengan keamanan teknis semata, tetapi juga mencakup persepsi publik terhadap niat baik dan tanggung jawab lembaga dalam mengelola data.

Dari perspektif komunikasi strategis, digital *trust* dibangun tidak hanya melalui sistem keamanan yang kuat, tetapi juga melalui cara lembaga berkomunikasi. Seperti dijelaskan oleh Kim, Ferrin, dan Rao (2008), kepercayaan dalam lingkungan digital sangat dipengaruhi oleh tiga faktor utama: kemampuan (*competence*), integritas (i*ntegrity*), dan niat baik (*benevolence*) dari organisasi. Ketiganya bisa dicapai melalui komunikasi yang konsisten, transparan, dan terbuka kepada publik, terutama saat terjadi krisis. Di sinilah peran humas menjadi sentral. Humas bukan sekadar menyampaikan informasi teknis, tetapi membangun dan mengelola narasi yang mencerminkan komitmen lembaga terhadap perlindungan data pribadi. Seperti dinyatakan oleh Botan dan Hazleton (2006), humas strategis bertujuan untuk menciptakan hubungan jangka panjang yang saling menguntungkan dengan publik melalui komunikasi yang berbasis kepercayaan dan keterlibatan aktif.

Dalam konteks kebocoran data, humas harus mampu menunjukkan bahwa lembaga bertanggung jawab, bersedia memperbaiki kesalahan, dan berkomitmen untuk meningkatkan keamanan di masa depan. Coombs (2007) juga menekankan bahwa kepercayaan publik dapat dibangun kembali melalui komunikasi krisis yang tepat termasuk permintaan maaf yang tulus, penyampaian fakta yang jujur, dan tindakan korektif yang nyata. Tanpa upaya ini, kepercayaan digital dapat hilang, dan dampaknya tidak hanya pada reputasi, tetapi juga pada loyalitas pengguna. Dengan demikian, digital *trust* bukanlah sesuatu yang dapat dibangun sekali jadi, melainkan hasil dari proses komunikasi strategis yang berkelanjutan, di mana humas memainkan peran kunci sebagai penjaga reputasi dan juru bicara institusi dalam menghadapi tantangan digital.

D. Etika Kehumasan dan Regulasi Perlindungan Data

Etika dalam kehumasan menekankan prinsip kejujuran, tanggung jawab sosial, dan kepatuhan terhadap hukum. Kode Etik IPRA (*International Public Relations Association*) mendorong praktisi humas untuk menyampaikan informasi yang tidak menyesatkan dan bersikap transparan, khususnya saat terjadi krisis. Di Indonesia, landasan hukum perlindungan data pribadi diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini menetapkan hak subjek data, kewajiban pengendali data, dan sanksi bagi pelanggaran. Namun, implementasinya menunjukkan tantangan praktis yang memengaruhi persepsi publik. Riset ini juga menyoroti rendahnya kesadaran masyarakat tentang hak-hak mereka dalam konteks perlindungan data, yang memperburuk krisis kepercayaan yang terjadi namun implementasinya menunjukkan tantangan praktis yang memengaruhi persepsi publik. Menurut Wiraguna (2024) rendahnya kesadaran masyarakat tentang hak-hak mereka dalam konteks perlindungan data, yang memperburuk krisis kepercayaan yang terjadi. Penerapan UU ini sangat relevan bagi praktisi humas yang terlibat dalam komunikasi terkait data pribadi, terutama dalam merespons krisis kebocoran data agar tetap sejalan dengan koridor hukum dan etika profesi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka (*library research*) dan analisis kasus (*case study*). Pendekatan kualitatif dipilih karena sesuai untuk menggali secara mendalam makna, peran, dan strategi humas dalam mengelola komunikasi krisis, khususnya dalam konteks kebocoran data pribadi yang memengaruhi kepercayaan publik. Studi kasus memungkinkan peneliti untuk memahami secara mendalam bagaimana institusi merespons insiden serangan siber dalam membentuk ulang citra di mata publik. Menurut Wiraguna dkk. (2024) bahwa studi kasus mampu menghadirkan pemahaman holistik terhadap fenomena digital kontemporer. Data yang digunakan dalam penelitian ini terdiri dari data sekunder yang diperoleh melalui berbagai literatur seperti jurnal ilmiah, buku teks, laporan media terpercaya, regulasi pemerintah, serta dokumen resmi lembaga terkait. Selain itu, data juga diperoleh dari studi kasus aktual mengenai kebocoran data pribadi di Indonesia, seperti kasus BPJS Kesehatan (2021) dan Bank Syariah Indonesia (2023).

Data dikumpulkan dengan cara dokumentasi, yaitu menelusuri dan mengkaji dokumen-dokumen yang relevan dengan topik penelitian, seperti laporan berita, artikel akademik, dan peraturan perundangan. Peneliti juga menelaah publikasi resmi dari institusi atau perusahaan yang pernah mengalami kebocoran data, guna mengetahui bagaimana strategi komunikasi krisis dijalankan oleh pihak humas. Teknik analisis data yang digunakan adalah analisis isi (*content analysis*) terhadap dokumen dan studi kasus yang telah dikumpulkan. Analisis ini dilakukan untuk mengidentifikasi pola komunikasi, strategi penanganan krisis, serta respons publik terhadap insiden kebocoran data. Hasil analisis kemudian dibandingkan dengan teori komunikasi krisis dan literatur terkait peran humas, untuk memperoleh simpulan yang mendalam dan relevan dengan permasalahan penelitian.

HASIL DAN PEMBAHASAN

A. Kebocoran Data BPJS Kesehatan (2021)

Pada bulan Mei 2021, Indonesia dikejutkan oleh kasus kebocoran data berskala besar yang melibatkan Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Sebanyak 279 juta data penduduk Indonesia, termasuk yang sudah meninggal dunia, diduga telah bocor dan diperjualbelikan di forum gelap (*dark web*). Data yang bocor mencakup informasi pribadi sensitif seperti Nomor Induk Kependudukan (NIK), nama lengkap, alamat, nomor telepon, email, dan bahkan data pekerjaan serta status kepesertaan BPJS. Skala kebocoran ini sangat masif dan mencakup hampir seluruh populasi, menjadikannya sebagai salah satu pelanggaran data terbesar dalam sejarah Indonesia. Dari segi komunikasi krisis, respons yang diberikan oleh BPJS Kesehatan dinilai tidak efektif dan tidak sesuai dengan prinsip-prinsip komunikasi publik dalam situasi darurat. Pada awalnya, BPJS bersikap defensif dan menyangkal adanya kebocoran data, bahkan ketika bukti digital mulai bermunculan dan diangkat oleh media massa serta praktisi keamanan siber. Lembaga baru memberikan klarifikasi resmi beberapa hari setelah kasus ini ramai diperbincangkan publik, yang menunjukkan keterlambatan dalam merespons krisis dan kurangnya kesiapan dalam menghadapi serangan reputasi.

Menurut *Situational Crisis Communication Theory* (SCCT) yang dikembangkan oleh Timothy Coombs (2007), organisasi yang secara jelas dianggap memiliki tanggung jawab atas terjadinya krisis (seperti dalam kategori *preventable crisis*) seharusnya menerapkan strategi komunikasi yang bersifat *accommodative*, seperti mengakui kesalahan (*apology*), menyediakan kompensasi (*corrective action*), dan menunjukkan empati kepada publik. Dalam konteks ini, BPJS seharusnya segera memberikan penjelasan terbuka, menjelaskan langkah pengamanan yang diambil, serta menyampaikan permohonan maaf secara resmi dan eksplisit. Namun, strategi yang dijalankan justru memperlihatkan minimnya transparansi, keterbukaan, dan empati, yang memperburuk persepsi publik. Alih-alih meningkatkan kepercayaan, respons yang terkesan tertutup dan lambat ini memicu krisis kepercayaan (*trust crisis*) terhadap BPJS

maupun lembaga pemerintah secara umum dalam hal pengelolaan data pribadi. Hal ini diperkuat oleh survei dari Katadata *Insight Center* (2021) yang menunjukkan bahwa lebih dari 60% responden merasa khawatir terhadap perlindungan data mereka setelah kasus tersebut mencuat.

Media juga memainkan peran penting dalam memperluas dampak krisis. Peliputan yang intens dan narasi kritis terhadap BPJS menyebabkan citra lembaga semakin tertekan. Dalam konteks ini, kegagalan BPJS untuk mengelola hubungan dengan media juga mencerminkan kelemahan dalam strategi humas dan komunikasi publiknya. Secara keseluruhan, kasus ini menunjukkan bahwa kegagalan dalam menerapkan prinsip komunikasi krisis dapat memperparah dampak reputasional dari sebuah insiden. Dalam era digital saat ini, keterlambatan dalam merespons dan kurangnya komunikasi yang strategis dapat dengan cepat menggerus digital *trust*, yang pada gilirannya memengaruhi legitimasi dan kredibilitas institusi di mata publik.

B. Serangan Siber terhadap Bank Syariah Indonesia (BSI) (2023)

Pada bulan Mei 2023, Bank Syariah Indonesia (BSI) menjadi korban serangan siber yang melumpuhkan sebagian besar sistem perbankan digitalnya. Layanan *mobile banking*, ATM, serta transaksi elektronik tidak dapat diakses oleh nasabah selama beberapa hari. Serangan ini diduga dilakukan oleh kelompok peretas asing yang menggunakan *ransomware LockBit* 3.0 dan mengklaim telah mencuri lebih dari 1,5 *terabyte* data, termasuk informasi nasabah, karyawan, dokumen internal, hingga rekaman transaksi. Kelompok tersebut bahkan mengancam akan mempublikasikan data jika tidak diberikan tebusan. Kasus ini segera mendapat perhatian luas, baik dari media, pakar keamanan siber, maupun masyarakat umum. Sebagai institusi keuangan besar dengan jutaan nasabah, gangguan ini menimbulkan kekhawatiran serius mengenai keamanan digital dan kepercayaan publik terhadap sistem perbankan nasional, khususnya yang dikelola oleh lembaga berbasis syariah.

Dari perspektif komunikasi krisis, respons awal dari pihak BSI dinilai tidak cukup cepat dan terbuka. Informasi resmi baru diberikan beberapa waktu setelah gangguan terjadi, dan penjelasan yang disampaikan dianggap terlalu teknis serta tidak menjawab kekhawatiran utama nasabah, yaitu keselamatan data pribadi dan dana mereka. Banyak nasabah menyuarakan kekecewaan di media sosial, menilai bahwa BSI tidak komunikatif dan terkesan menutupi skala insiden. Menurut prinsip *Situational Crisis Communication Theory* (SCCT), organisasi yang mengalami serangan siber dengan dampak signifikan pada publik, meskipun termasuk dalam kategori *victim cluster* (di mana organisasi tidak sepenuhnya bertanggung jawab atas kejadian), tetap perlu menjalankan strategi komunikasi yang informatif dan empatik. Hal ini termasuk penyampaian fakta secara berkala, jaminan kepada nasabah mengenai langkah pemulihan, serta komunikasi dua arah melalui kanal resmi dan media sosial.

Dalam kasus BSI, strategi komunikasi yang dilakukan dinilai kurang optimal. Tidak ada permintaan maaf publik yang eksplisit sejak awal, dan tidak semua pertanyaan publik dijawab secara terbuka. Namun, perlu dicatat bahwa dalam tahap selanjutnya, BSI berusaha melakukan pemulihan reputasi dengan menggandeng Badan Siber dan Sandi Negara (BSSN), melakukan audit keamanan, serta memperkuat sistem teknologi informasi. Upaya ini menunjukkan adanya niat perbaikan, tetapi tetap tidak sepenuhnya menutupi kekurangan dalam manajemen komunikasi awal krisis, yang seharusnya menjadi fokus utama peran humas.

Kasus ini mempertegas pentingnya kesiapsiagaan humas dalam menghadapi krisis digital, terutama dalam sektor sensitif seperti keuangan. Di era digital, keterlambatan dan minimnya transparansi dalam komunikasi bukan hanya memperburuk citra institusi, tetapi juga dapat memicu kepanikan dan perpindahan loyalitas publik ke institusi lain yang dianggap lebih aman dan terpercaya.

C. Perbandingan Strategi dan Implikasi terhadap Citra Institusi

Perbandingan antara kasus kebocoran data BPJS Kesehatan (2021) dan serangan siber terhadap Bank Syariah Indonesia (2023) menunjukkan bahwa strategi komunikasi krisis yang dijalankan oleh suatu institusi sangat memengaruhi tingkat keberhasilan dalam menjaga dan memulihkan citra lembaga. Dalam kedua kasus tersebut, krisis yang terjadi sama-sama menyangkut pelanggaran terhadap privasi dan keamanan data pribadi, namun pendekatan komunikasi yang diambil berbeda dalam hal kecepatan, transparansi, serta kualitas keterlibatan dengan publik.

Pada kasus BPJS Kesehatan, komunikasi yang lambat, defensif, dan tidak akuntabel memperburuk persepsi publik. Masyarakat merasa informasi disembunyikan, dan tidak ada tanggung jawab yang jelas dari institusi. Strategi ini bertolak belakang dengan teori *Situational Crisis Communication Theory* (SCCT) yang menekankan pentingnya strategi akomodatif terutama dalam krisis yang melibatkan kesalahan internal atau kelemahan sistem yang bisa diantisipasi. Ketidakhadiran komunikasi empatik dan permintaan maaf dari BPJS memperdalam krisis kepercayaan masyarakat terhadap lembaga negara.

Sementara itu, meskipun BSI juga menghadapi kritik karena keterlambatan informasi, lembaga ini menunjukkan respons perbaikan dengan melibatkan BSSN, memperkuat sistem TI, dan memberikan pernyataan publik dalam tahap pemulihan. Walaupun langkah ini tidak sepenuhnya memulihkan kepercayaan nasabah, upaya pemulihan reputasi yang dilakukan mencerminkan adanya kesadaran humas terhadap pentingnya memperbaiki citra jangka panjang. Menurut Fearn-Banks (2024) dalam *Crisis Communications*, keberhasilan komunikasi krisis tidak hanya diukur dari bagaimana institusi bereaksi saat krisis berlangsung, tetapi juga dari bagaimana mereka mengelola narasi dan pemulihan reputasi setelah krisis mereda.

Dari perbandingan ini, dapat disimpulkan bahwa keterbukaan, kecepatan merespons, dan sikap empatik adalah tiga elemen kunci dalam membangun digital *trust* di tengah krisis. Ketika komunikasi dilakukan secara jujur dan proaktif, publik lebih cenderung memberi ruang bagi institusi untuk memperbaiki kesalahan, bahkan tetap mempertahankan loyalitas terhadap institusi tersebut. Sebaliknya, jika komunikasi bersifat tertutup, defensif, atau terkesan menyalahkan pihak lain, maka kerusakan citra bisa bersifat jangka panjang, dan kepercayaan publik sangat sulit untuk dipulihkan.

Dalam konteks ini, humas tidak hanya berperan sebagai penyampai informasi, tetapi menjadi aktor utama dalam mengelola persepsi, membangun kepercayaan, dan menjaga kredibilitas organisasi. Sebagaimana ditegaskan oleh Grunig dan Hunt (2005) dalam *Managing Public Relations*, humas strategis harus mampu bertindak sebagai penghubung antara kepentingan publik dan organisasi, terlebih saat terjadi krisis. Di tengah era digital yang ditandai oleh kecepatan arus informasi dan tingginya ekspektasi publik terhadap transparansi, peran humas sebagai fasilitator komunikasi krisis yang etis dan strategis menjadi semakin vital dan tidak dapat diabaikan.

D. Tantangan Humas dalam mengelola Citra Institusi di tengah Isu Serangan Siber dan Kebocoran Data

Dalam menghadapi krisis kebocoran data pribadi, humas tidak hanya berhadapan dengan tantangan teknis dalam menyampaikan informasi, tetapi juga dengan dinamika organisasi internal, tekanan eksternal dari publik, dan ekspektasi sosial yang tinggi terhadap transparansi serta akuntabilitas. Salah satu tantangan utama adalah minimnya koordinasi internal antara tim teknologi informasi (TI) dan tim komunikasi. Dalam banyak kasus, termasuk pada insiden BPJS Kesehatan dan BSI, terdapat keterlambatan dalam penyampaian informasi karena tidak adanya jalur komunikasi yang jelas antara pihak yang mengetahui teknis insiden (TI) dan pihak yang bertugas menyampaikannya ke publik (humas). Hal ini menyebabkan ketidaksinkronan pesan, keterlambatan klarifikasi, dan bahkan kebingungan informasi di ruang publik.

Selain itu, humas dihadapkan pada tekanan besar dari publik dan media sosial, di mana masyarakat menuntut respons yang cepat, jujur, dan solutif. Di era digital, keterlambatan memberikan pernyataan resmi bahkan hanya dalam hitungan jam dapat menimbulkan spekulasi, opini negatif, dan viralnya informasi yang tidak akurat. Seperti yang dijelaskan oleh Fearn-Banks (2016), dalam situasi krisis, kecepatan dan ketepatan dalam menyampaikan pesan sangat menentukan arah opini publik dan kepercayaan terhadap lembaga.

Tantangan lainnya adalah tidaknya adanya regulasi internal atau protokol baku terkait manajemen komunikasi dalam kasus kebocoran data. Banyak lembaga belum memiliki standar operasional prosedur (SOP) khusus yang mengatur bagaimana humas harus bertindak saat terjadi pelanggaran data. Akibatnya, ketika krisis muncul secara tiba-tiba, humas bekerja tanpa pedoman yang jelas dan cenderung bersikap reaktif daripada strategis. Hal ini juga menunjukkan pentingnya kesiapsiagaan institusi dalam membangun sistem manajemen risiko komunikasi yang terintegrasi dengan sistem keamanan data.

Yang tidak kalah penting, humas juga harus menghadapi krisis kepercayaan digital (*digital trust crisis*). Setelah insiden kebocoran data, masyarakat cenderung menjadi skeptis terhadap semua bentuk pernyataan institusi, terutama janji-janji terkait keamanan data dan privasi. Ini menjadi beban psikologis dan reputasional yang harus dikelola oleh tim komunikasi dengan sangat hati-hati. Menurut *World Economic Forum* (2020), membangun kembali kepercayaan digital memerlukan komitmen jangka panjang yang ditunjukkan melalui transparansi, tindakan nyata, serta keterlibatan publik dalam proses pemulihan.

Untuk mengatasi tantangan-tantangan tersebut, diperlukan langkah sistematis dan berkelanjutan. Institusi harus mulai menyusun pedoman komunikasi krisis berbasis risiko data, mengintegrasikan tim TI dan humas dalam satu sistem respons cepat, serta membekali praktisi humas dengan pelatihan khusus mengenai perlindungan data pribadi, manajemen insiden siber, dan komunikasi publik berbasis empati. Lebih dari itu, prinsip transparansi harus dijadikan nilai utama dalam setiap tindakan komunikasi saat terjadi krisis, agar masyarakat tidak merasa dikhianati dan tetap mempertahankan kepercayaan terhadap institusi.

KESIMPULAN

Penelitian ini menyoroti peran sentral humas dalam mengelola komunikasi krisis di tengah isu kebocoran data pribadi yang kian marak di Indonesia. Melalui studi kasus kebocoran data BPJS Kesehatan (2021) dan serangan siber terhadap Bank Syariah Indonesia (2023), dapat disimpulkan bahwa efektivitas strategi komunikasi sangat memengaruhi tingkat kepercayaan publik terhadap institusi. Institusi yang gagal menunjukkan keterbukaan, tanggung jawab, dan empati dalam merespons krisis cenderung kehilangan kepercayaan publik secara drastis, seperti yang terjadi pada BPJS. Sebaliknya, BSI yang lambat namun kemudian menggunakan pendekatan permintaan maaf dan tindakan korektif, sedikit lebih mampu mengelola persepsi publik. Dalam konteks ini, metode komunikasi krisis yang paling relevan dan terbukti efektif adalah strategi *rebuild* dari teori *Situational Crisis Communication Theory (SCCT)* yang dikembangkan oleh Timothy Coombs. Metode ini menekankan pentingnya pengakuan (*apology*), transparansi informasi, dan aksi korektif nyata sebagai langkah awal pemulihan kepercayaan. Strategi ini sangat tepat digunakan dalam krisis yang sifatnya *preventable*, yaitu krisis yang muncul akibat kelalaian atau kesalahan institusi yang seharusnya bisa dicegah, seperti dalam kasus kebocoran data akibat lemahnya keamanan sistem.

Strategi *rebuild* bukan hanya metode komunikasi, tetapi juga pendekatan hubungan masyarakat yang menempatkan empati, akuntabilitas, dan keterbukaan sebagai landasan utama. Penggunaan metode ini tidak hanya mampu memulihkan reputasi secara jangka pendek, tetapi juga berpotensi membangun kembali kepercayaan digital yang bersifat jangka panjang, terutama jika disertai dengan reformasi sistem dan pelibatan publik dalam proses transparansi. Dengan demikian, dapat disimpulkan bahwa dalam era digital yang penuh risiko siber, metode

komunikasi krisis berbasis *rebuild* adalah pilihan terbaik bagi humas untuk menjaga keberlanjutan hubungan institusi dengan publik. Strategi ini bukan hanya respons terhadap krisis, tetapi juga investasi terhadap kepercayaan masa depan.

DAFTAR PUSTAKA

BPJS Kesehatan. (2021). *Pernyataan resmi terkait dugaan kebocoran data peserta*. https://www.bpjs-kesehatan.go.id/

CNBC Indonesia. (2023, Mei 10). "BSI diserang ransomware, nasib uang nasabah gimana?" CNBC Indonesia. https://www.cnbcindonesia.com/tech/20230510174928-37-436279/bsi-diserang-ransomware-nasib-uang-nasabah-gimana

Coombs, W. T. (2007). *Ongoing crisis communication: Planning, managing, and responding* (2nd ed.). Sage Publications.

Cutlip, S. M., Center, A. H., & Broom, G. M. (2009). *Effective public relations* (11th ed.). Pearson Education.

Fearn-Banks, K., & Kawamoto, K. (2024). *Crisis communications: A casebook approach* (6th ed.). Routledge.

Fombrun, C. J., & Van Riel, C. B. M. (2004). *Fame and fortune: How successful companies build winning reputations*. FT Press.

Greenleaf, G. (2017). "Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey". *Privacy Laws & Business International Report, 145*, 10–13.

Grunig, J. E., & Hunt, T. (1984). *Managing public relations*. Holt, Rinehart and Winston.

Harlow, R. F. (1976). "Building a public relations definition". *Public Relations Review, 2*(4), 34–42. https://doi.org/10.1016/S0363-8111(76)80008-3

IBM Security. (2022). *Cost of adata breach report 2022*. https://www.ibm.com/reports/data-breach

Katadata Insight Center. (2023, November 10). "Pelindungan data pribadi warga RI masih tergolong rendah". Databoks by Katadata.co.id. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/2e2c8c8e1e87fdf/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah

Kompas.com. (2023, May 11). "Bank Syariah Indonesia alami gangguan layanan akibat serangan siber". https://money.kompas.com/read/2023/05/11/

Metro TV News. (2024). "Indonesia di posisi 3 negara dengan kebocoran data terbanyak". https://www.metrotvnews.com/play/bD2CZ6Wp-indonesia-di-posisi-3-negara-dengan-kebocoran-data-terbanyak

Solove, D. J. (2006). "A taxonomy of privacy". *University of Pennsylvania Law Review, 154*(3), 477–560. https://doi.org/10.2307/40041279

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2010). *Effective crisis communication: Moving from crisis to opportunity* (2nd ed.). Sage Publications.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Wiraguna, S. A., Purwanto, L. M. F., & Widjaja, R. R. (2024). "Metode penelitian kualitatif di era transformasi digital". *Arsitekta: Jurnal Arsitektur dan Kota Berkelanjutan, 6*(1), 46–60. https://doi.org/10.18860/jia.v4i1.3466

Sulaiman, A., & Barthos, M. (2024). "Implementation of consumer personal data protection in ecommerce from the perspective of Law No. 27 of 2022". *Journal of World Science, 3*(3), 410–418. https://doi.org/10.58905/jws.v3i3.103

World Economic Forum. (2020). *The global risks report 2020*. https://www.weforum.org/reports/the-global-risks-report-2020

World Economic Forum. (2020). *Advancing digital trust: A cybersecurity guide for business leaders*. https://www.weforum.org/reports/advancing-digital-trust-a-cybersecurity-guide-for-business-leaders