Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 753-760

DEKONSTRUKSI PATOLOGI KOMUNIKASI DIGITAL: TAKTIK SOSIOLINGUISTIK DAN EKSPLOITASI KERENTANAN KOGNITIF PADA KASUS REKAYASA SOSIAL DI PLATFORM PESAN INSTAN

Rhevalino Armadyta Putra[1], Delilah Sancaka Mahesa[2] Berliana Aulia[3], Nazwa Maulida Darimi[4], Zalfa Adhwa Nafisa[5], M. Rofi Akbar[6], M. Restu Hafiz Dharmawan[7]
Program Studi Public Relations, Fakultas Ilmu Komunikasi, Universitas Esa Unggul[1,2,3,4,5,6,7]
E-mail: rhevalinoaarmadyta@gmail.com[1] ,adelmahesa11@gmail.com[2], berlianaaulia01@gmail.com[3], nzwamlda@gmail.com[4], zalfadhwa@gmail.com[5], muhammadrofiakbar15@gmail.com [6], restuhafiz24@gmail.com[7]

Informasi

Volume : 3
Nomor : 7
Bulan : Juli
Tahun : 2026
E-ISSN : 3062-9624

Abstract

Pesatnya perkembangan teknologi digital turut memicu maraknya kejahatan siber berbasis manipulasi psikologis, seperti modus penipuan berkedok kurir paket melalui WhatsApp. Penelitian ini bertujuan untuk membedah anatomi dari skenario jebakan tersebut dengan memadukan pendekatan sosiologi komunikasi dan psikologi komunikasi. Metode yang digunakan adalah studi literatur kualitatif dengan menelaah berbagai artikel ilmiah yang diterbitkan sepanjang tahun 2020 hingga 2026. Hasil analisis menunjukkan bahwa pelaku penipuan menggunakan taktik bahasa yang terstruktur secara sistematis, mulai dari membangun otoritas semu, menaikkan tensi urgensi, hingga melakukan eksekusi fatal. Secara sosiologis, pelaku mendompleng nama besar penyedia jasa ekspedisi resmi untuk menciptakan relasi kuasa yang timpang dan meruntuhkan benteng kepercayaan korban. Sementara dari sisi psikologis, kombinasi ancaman dan manipulasi rasa penasaran sengaja diciptakan untuk memicu kelelahan otak (*cognitive overload*). Kondisi tertekan ini memaksa korban mengambil keputusan secara instan (*heuristik*) dan mengabaikan logika analitisnya. Penelitian ini menyimpulkan perlunya perombakan paradigma literasi digital di Indonesia; edukasi tidak boleh lagi hanya berfokus pada aspek teknis, melainkan harus bergeser ke arah pemahaman perilaku demi membangun imunitas kognitif masyarakat yang lebih kuat.

Kata Kunci: Rekayasa Sosial, Penipuan WhatsApp, Sosiologi Komunikasi, Psikologi Komunikasi, Imunitas Kognitif

Abstract

The rapid advancement of digital technology has fueled the rise of psychological manipulation-based cybercrimes, such as the package delivery scam on WhatsApp. This study aims to dissect the anatomy of such deceptive scenarios by integrating the sociology of communication and the psychology of communication. Employing a qualitative literature review design, this study analyzes various scholarly articles published between 2020 and 2026. The findings reveal that perpetrators employ systematically structured linguistic tactics, encompassing the establishment of pseudo-authority, the escalation of urgency, and fatal execution. From a sociological standpoint, perpetrators leverage the reputation of official delivery services to construct asymmetrical power relations and breach the victim's trust framework. Psychologically, a combination of manufactured threats and curiosity manipulation is deliberately deployed to induce cognitive overload. This high-pressure state forces victims to process

information heuristically, making instantaneous decisions while bypassing analytical rationality. This study underscores the urgent need to overhaul Indonesia's digital literacy paradigm; education must transcend technical skills and shift toward behavioral insights to foster robust cognitive immunity among the public.

Keywords: *Social Engineering, WhatsApp Scams, Sociology of Communication, Psychology of Communication, Cognitive Immunity.*

A. PENDAHULUAN

Lompatan teknologi informasi yang begitu cepat belakangan ini telah merombak total pola interaksi sosial masyarakat. Pergeseran ini memang menawarkan efisiensi tinggi, namun di sisi lain melahirkan efek samping berupa penyimpangan perilaku di ruang siber—sebuah patologi komunikasi digital. Di Indonesia, bentuk yang paling merusak dan kerap memakan korban adalah kejahatan berbasis rekayasa sosial (*social engineering*) lewat aplikasi pesan instan seperti WhatsApp. Modus penipuan berkedok kurir paket kini bertransformasi menjadi ancaman yang memiliki banyak wajah. Pelaku biasanya mengirimkan berkas berbahaya berformat aplikasi Android (.apk) atau tautan manipulatif dengan menyamar sebagai kurir dari perusahaan ekspedisi resmi.

Taktik ini secara jeli mengeksploitasi ketergantungan masyarakat modern terhadap ekosistem belanja daring. Kita seolah dikondisikan untuk selalu memiliki ekspektasi bahwa akan ada paket yang datang. Walaupun ujung dari penipuan ini bermuara pada kerugian finansial yang teknis seperti peretasan akun perbankan pintu masuk keberhasilan mereka sepenuhnya bertumpu pada kemanjuran pesan teks yang dikirimkan. Ketika korban gagal mendeteksi kejanggalan dalam komunikasi digital tersebut, di situlah seluruh benteng keamanan data pribadi mulai runtuh.

Jika dibedah menggunakan sosiologi komunikasi, efektivitas penipuan ini bersumber dari kelihaian pelaku dalam mengonstruksi realitas palsu melalui medium teks. Penipu modern tidak lagi sekadar menyebar pesan acak secara membabi buta. Mereka merancang skenario interaksi yang sangat terstruktur demi membangun otoritas dan legitimasi semu di mata korban. Pola ini sejalan dengan premis Dave (2025) mengenai komunikasi manipulatif dalam kejahatan siber, yang menyatakan bahwa arsitektur penipuan digital kontemporer sangat bergantung pada siasat linguistik yang dirancang khusus untuk mengikis kecurigaan target hingga titik terendah.

Melalui kemampuan meniru gaya bahasa kurir yang formal, penggunaan sapaan kehumasan yang santun, hingga pemanfaatan atribut visual logistik resmi, pelaku berhasil meretas ruang kepercayaan personal di WhatsApp. Taktik linguistik ini tidak lagi sekadar menjadi alat penyampai pesan, melainkan bermutasi menjadi instrumen kendali yang menempatkan korban dalam relasi kuasa yang timpang. Dalam situasi penuh kepalsuan ini, korban dikondisikan untuk patuh pada instruksi kebahasaan yang didiktekan oleh penipu yang memegang kendali penuh atas arus informasi.

Namun, dominasi bahasa tersebut tidak akan berjalan mulus tanpa adanya penetrasi yang menyasar sisi psikologis korban. Berdasarkan kerangka rekayasa sosial dalam

keamanan siber, celah keberhasilan modus kurir palsu ini terbuka karena adanya keselarasan antara metode serangan dengan titik lemah psikologis manusia. Pelaku merekayasa stimulus pesan teks untuk memicu lonjakan emosi yang drastis melalui dua instrumen utama.

Pertama adalah pemanfaatan rasa takut, di mana pelaku membangun narasi bahwa paket akan ditahan, dikembalikan, atau hangus jika tidak segera dikonfirmasi. Kedua adalah eksploitasi rasa penasaran lewat teka-teki mengenai kondisi fisik paket yang diklaim rusak parah. Tekanan emosional yang datang bertubi-tubi dalam waktu singkat ini memicu beban kognitif berlebih (cognitive overload) pada otak korban. Akibatnya, sistem pemrosesan informasi terpaksa beralih ke mode cepat atau heuristik, sehingga fungsi berpikir kritis-analitis mengalami kelumpuhan sesaat. Dalam kondisi kehilangan rasionalitas itulah, tindakan fatal seperti mengunduh berkas berbahaya dilakukan secara impulsif tanpa adanya verifikasi ulang yang jernih.

Meskipun ruang diskusi mengenai keamanan digital di Indonesia sudah banyak dieksplorasi, penelusuran literatur menunjukkan adanya kekosongan fokus yang cukup signifikan. Mayoritas penelitian terdahulu cenderung terjebak pada pendekatan hukum pidana positif yang berfokus pada regulasi, atau pendekatan teknik informatika yang menitikberatkan pada forensik digital dan keamanan jaringan komputer. Masih sangat sedikit publikasi yang menempatkan teks serta dinamika interaksi psikologis sebagai objek utama yang dibedah secara interdisipliner.

Kebaruan ilmiah dari penelitian ini justru terletak pada upaya membongkar akar masalah penipuan siber melalui perpaduan dua pisau analisis sekaligus: sosiologi komunikasi untuk memetakan taktik linguistik pelaku, dan psikologi komunikasi untuk mengidentifikasi celah kerentanan kognitif korban. Mengabaikan aspek komunikasi ini hanya akan membuat seluruh rancangan program literasi digital masyarakat berhenti di permukaan. Selama ini masyarakat hanya diajari cara mengenali virus digitalnya, tanpa pernah disadarkan bagaimana logika mereka bisa dimanipulasi dengan mudah oleh struktur bahasa.

Berangkat dari urgensi teoretis tersebut, penelitian ini merumuskan masalah pada bagaimana struktur taktik bahasa pelaku memengaruhi kesadaran korban, serta bagaimana dampak psikologis dari pesan tersebut mampu melumpuhkan nalar rasional. Oleh karena itu, penelitian kualitatif ini bertujuan untuk mendekonstruksi secara utuh taktik rekayasa sosial dalam kasus penipuan paket di WhatsApp melalui metode analisis teks interpretatif. Secara praktis, hasil dekonstruksi ini diharapkan bisa menjadi landasan kuat dalam menyusun modul edukasi literasi digital berbasis wawasan perilaku (behavioral insights). Tujuannya agar masyarakat memiliki imunitas kognitif yang kokoh sehingga tidak mudah terjebak oleh manipulasi bahasa di ruang digital.

B. METODE PENELITIAN

Penelitian ini menerapkan desain studi literatur kualitatif dengan pendekatan deskriptif analitis untuk membedah mekanisme rekayasa sosial pada penipuan berkedok kurir paket di WhatsApp. Pilihan metode ini didasari keinginan untuk menelaah, menyaring, dan menyintesis data teks secara kritis agar fenomena patologi komunikasi bisa dipahami secara substansial, tanpa perlu terikat pada pengujian hipotesis statistik. Proses riset berlangsung

selama empat bulan, dari Maret hingga Juni 2026, yang seluruhnya digarap di ruang digital dengan mengakses pangkalan data bereputasi seperti SINTA, Google Scholar, ScienceDirect, dan ResearchGate. Populasi data mencakup artikel jurnal ilmiah, prosiding konferensi, serta buku teks akademik terbitan tahun 2020 sampai 2026. Penentuan sampelnya menggunakan teknik purposive sampling dengan kriteria inklusi yang ketat; literatur wajib mengulas dimensi sosiologi atau psikologi komunikasi serta relevan dengan konteks platform pesan instan. Dari hasil penyaringan tersebut, dipilihlah dua jurnal acuan utama—termasuk kajian dari Dave (2025) serta sepuluh artikel pendukung sebagai korpus data inti.

Pengumpulan data dijalankan lewat dokumentasi sistematis, dimulai dari penelusuran masif menggunakan kombinasi kata kunci khusus seperti rekayasa sosial, taktik linguistik, WhatsApp, psikologi komunikasi, dan literasi kejahatan siber. Setelah menyaring judul dan abstrak, peneliti membedah kelayakan isinya secara utuh untuk memastikan kedalaman teoretis setiap literatur yang terpilih. Argumen kunci dan temuan empiris yang lolos kurasi kemudian diekstraksi ke dalam matriks kategorisasi analisis konseptual. Selanjutnya, data diolah menggunakan metode analisis isi kualitatif yang dikombinasikan dengan analisis tematik lewat model siklus interaktif Miles, Huberman, dan Saldana. Proses ini berjalan dalam tiga alur simultan: reduksi data untuk memilah aspek taktik komunikasi pelaku dan kerentanan psikologis korban; penyajian data untuk mengomparasikan konsep taktik linguistik milik Dave (2025) dengan teori keamanan rekayasa sosial; serta penarikan kesimpulan melalui interpretasi mendalam yang divalidasi dengan *grand theory* demi menjaga keabsahan ilmiah dari dekonstruksi teks yang dilakukan.

C. HASIL DAN PEMBAHASAN

Hasil Penelitian

Dari perpaduan sintesis data kualitatif dan analisis empiris terhadap isi chat penipuan kurir paket di WhatsApp, riset ini membongkar fakta bahwa rekayasa sosial di ruang digital sama sekali tidak bergerak secara acak atau asal-asalan. Aksi ini justru berjalan lewat skenario komunikasi yang sangat matang dan terhitung secara presisi. Secara anatomi, modus penipuan ini bekerja mirip sebuah mesin yang mempertemukan dua komponen penggerak utama: stimulus eksternal berupa siasat bahasa (linguistik), dan respons internal berupa eksploitasi pada celah fungsi kognitif manusia.

Seluruh hasil dekonstruksi taktik operasional tersebut telah dipetakan secara runut ke dalam tiga fase interaksi manipulatif, yang disajikan secara lengkap pada Tabel 1.

Tabel 1. Pemetaan Dekonstruksi Taktik Rekayasa Sosial pada Penipuan WhatsApp

Tahapan Interaksi	Taktik Linguistik (Sosiologi Komunikasi)	Kerentanan Sasaran (Psikologi Komunikasi)
Inisiasi Otoritas Semu	Pelaku meniru identitas sosial sebagai kurir ekspedisi melalui sapaan formal, istilah logistik resmi, dan klaim keterkaitan dengan perusahaan pengiriman.	Korban cenderung percaya karena terbiasa menerima informasi pengiriman paket dari pihak ekspedisi.

Eskalasi Urgensi	Pelaku menggunakan diksi ancaman waktu, misalnya paket akan diretur, tertahan, atau hangus apabila tidak segera dikonfirmasi.	Kecemasan meningkat secara cepat sehingga beban kognitif bertambah dan daya nalar korban melemah.
Eksekusi Fatal	Pelaku memberi instruksi langsung agar korban membuka dokumen aplikasi, tautan foto, atau lampiran yang seolah berkaitan dengan paket.	Korban terdorong bertindak impulsif karena rasa takut dan penasaran, sehingga berpikir cepat secara heuristik dan mengabaikan verifikasi.

Pemetaan di atas memperlihatkan dengan sangat jelas bahwa file aplikasi berbahaya itu sebenarnya cuma alat teknis di babak akhir. Senjata paling mematikan dari penipu justru terletak pada tahap awal: bagaimana mereka membangun otoritas semu dan sengaja memicu kepanikan. Secara sosiologis, pelaku membajak norma interaksi yang biasa kita gunakan sehari-hari untuk melumpuhkan akal sehat korban langsung dari dalam pikirannya sendiri.

Pembahasan

Rincian temuan riset ini dibedah lebih jauh menggunakan gabungan dua perspektif keilmuan. Pendekatan ini diambil demi menyajikan gambaran yang utuh mengenai bagaimana sebaris pesan teks pendek mampu memicu tindakan fatal yang berujung pada kerugian besar di pihak korban.

Dekonstruksi Taktik Linguistik: Perspektif Sosiologi Komunikasi

Lewat kacamata sosiologi komunikasi, bahasa punya peran yang jauh lebih dalam dari sekadar alat bertukar pesan; ia bisa menjelma menjadi instrumen kekuasaan untuk menyetir cara pandang seseorang terhadap realitas. Temuan dalam riset ini sangat sejalan dengan pandangan Dave (2025) mengenai komunikasi manipulatif. Menurutnya, penipu siber zaman sekarang sering kali bertingkah layaknya seorang sosiolog. Mereka secara aktif memanfaatkan norma kesopanan yang biasa berlaku sehari-hari untuk merajut realitas buatan yang terlihat sangat meyakinkan.

Pada tahap awal, pelaku mulai menyamar dengan meniru habis cara berkomunikasi seorang kurir. Mereka dengan jeli menyelipkan istilah-istilah khas dunia logistic seperti "nomor resi" atau "estimasi pengantaran" ditambah sapaan formal penuh hormat seperti "Bapak" atau "Ibu". Ini adalah taktik bahasa yang sengaja disusun demi menciptakan kesan bahwa mereka memiliki otoritas resmi. Secara sosiologis, kita sejak kecil sudah dibentuk oleh lingkungan untuk patuh dan percaya pada lembaga formal. Jadi, begitu penipu membungkus diri mereka dengan gaya bahasa khas ekspedisi besar, mereka sebenarnya sedang menumpang hidup pada rasa percaya yang sudah tertanam kuat di tengah masyarakat.

Jika dibedah lebih dalam menggunakan teori Konstruksi Realitas Sosial dari Peter L. Berger dan Thomas Luckmann, manipulasi pikiran seperti ini terasa sangat masuk akal. Di ruang obrolan digital yang miskin isyarat nonverbal, untaian teks otomatis menjadi satu-satunya penentu realitas di kepala kita. Di sini, penipu sengaja menciptakan ketimpangan informasi di mana hanya mereka yang memegang kendali atas jalannya obrolan. Ketika mereka mulai memakai kalimat perintah di detik-detik akhir menjelang eksekusi, itulah wujud nyata dari dominasi komunikasi. Korban seolah terseret masuk ke dalam jebakan relasi

kuasa tersebut, hingga akhirnya menuruti kemauan pelaku secara spontan tanpa sempat berpikir untuk mengecek ulang kebenaran informasinya ke pihak ekspedisi yang asli.

Tambahan penting dari bagian ini adalah bahwa kekuatan bahasa penipu tidak hanya muncul dari pilihan kata yang terdengar resmi, tetapi juga dari kemampuannya membaca kebiasaan sosial masyarakat digital. Banyak orang saat ini sudah terbiasa menerima pesan singkat dari kurir, admin toko daring, atau layanan ekspedisi tanpa proses verifikasi yang panjang. Kebiasaan inilah yang dimanfaatkan pelaku sebagai jalan masuk. Mereka tidak perlu membangun kepercayaan dari nol, karena kepercayaan itu sebenarnya sudah tersedia dalam pola hidup masyarakat yang makin bergantung pada transaksi digital. Dengan kata lain, penipuan ini bekerja karena pelaku berhasil menyatu dengan rutinitas komunikasi sehari-hari korban.

Eksploitasi Kerentanan Kognitif: Perspektif Psikologi Komunikasi

Keberhasilan telak dari manipulasi bahasa di atas tidak akan terjadi jika kondisi psikologis korban kebal terhadap intervensi emosional. Kenyataan ini sangat berkaitan dengan konsep rekayasa sosial (social engineering) dalam keamanan siber, yang menyebutkan bahwa serangan digital yang presisi selalu mengincar titik lemah kognitif yang melekat pada sifat alami manusia.

Dari sudut pandang psikologi, mulusnya skema penipuan di WhatsApp ini bisa dibedah menggunakan Teori Proses Ganda (Dual Process Theory) tentang bagaimana otak manusia memproses informasi. Dalam situasi normal yang tenang, kita biasanya mencerna informasi mencurigakan dengan mengaktifkan Sistem 2 mode berpikir analitis yang bekerja lambat, penuh kehati-hatian, dan membutuhkan energi mental yang besar.

Namun, penipu tahu betul cara merusak ritme berpikir tersebut lewat sengatan emosional. Mereka memberondong korban dengan kalimat ancaman terkait batas waktu atau risiko kehilangan barang demi memicu rasa takut yang instan. Lonjakan kecemasan yang tiba-tiba ini langsung memenuhi kapasitas otak hingga memicu beban kognitif berlebih (cognitive overload). Dalam kondisi yang mendesak dan penuh tekanan psikologis, otak korban otomatis menyalakan alarm darurat dengan memutus jalur Sistem 2 yang lambat, lalu mengalihkan kemudi sepenuhnya ke Sistem 1. Sistem ini bekerja lewat jalan pintas mental (heuristik) yang sangat terburu-buru, otomatis, dan murni digerakkan oleh luapan emosi.

Di titik runtuhnya rasionalitas inilah kerentanan psikologis korban mencapai puncaknya. Pikiran yang sudah dikuasai oleh mode heuristic ditambah rasa penasaran akibat skenario paket yang diklaim rusak membuat korban langsung mengklik dan mengunduh file aplikasi berbahaya tersebut secara impulsif. Fungsi analitis mereka lumpuh total, sehingga mereka gagal menyadari kejanggalan yang sangat mencolok: bahwa format file aplikasi (.apk) sama sekali tidak masuk akal untuk sebuah foto atau dokumen bukti pengiriman.

Dampak destruktif dari manipulasi kognitif ini juga didukung kuat oleh fenomena psikologis yang sering terjadi di aplikasi pesan privat seperti WhatsApp, yaitu bias kebenaran (truth bias). Fenomena ini menjelaskan kecenderungan alami manusia untuk langsung memercayai pesan dari orang lain sebagai kebenaran di awal interaksi. Sifat WhatsApp yang terasa personal dan dekat di ponsel pribadi berhasil memangkas rasa curiga korban secara

drastis, sangat berbeda jika pesan serupa diterima melalui email korporat formal yang secara otomatis memicu kewaspadaan kita.

Dalam kondisi seperti ini, korban sebenarnya tidak selalu kurang pengetahuan soal keamanan digital. Sering kali mereka tahu bahwa tautan mencurigakan atau file asing berisiko, tetapi pengetahuan itu kalah cepat dibanding tekanan emosional yang sedang mereka rasakan. Rasa takut kehilangan paket, khawatir dianggap lalai, atau sekadar penasaran terhadap isi lampiran membuat keputusan diambil dalam hitungan detik. Di sinilah terlihat bahwa literasi digital tidak cukup hanya mengajarkan aturan teknis, melainkan juga perlu melatih kemampuan menunda respons. Jeda beberapa detik untuk bertanya, mengecek nomor resmi, atau tidak langsung mengikuti instruksi bisa menjadi benteng sederhana yang sangat menentukan.

D. KESIMPULAN

Sintesis mendalam dari kedua perspektif di atas bermuara pada kesimpulan penting yang membawa implikasi teoretis serta praktis yang kuat. Secara teoretis, berbagai temuan dalam kajian ini menegaskan kembali bahwa wabah patologi komunikasi digital saat ini tidak boleh dipandang sebatas masalah teknis atau kegagalan teknologi. Ini adalah persoalan mundurnya interaksi kognitif sosial yang bersifat sistemik. Kita sedang menyaksikan evolusi nyata di mana kejahatan siber telah bergeser; dari yang dulunya berupa peretasan sistem komputer yang rumit, kini bertransformasi menjadi seni meretas sisi lemah kognisi dan psikologis manusia.

Secara praktis, analisis ini memberikan masukan penting bagi kebijakan publik, terutama mengenai urgensi perombakan paradigma dalam kampanye literasi digital yang digalakkan pemerintah. Menyelesaikan benang kusut penipuan digital tidak akan memberikan dampak luas jika pemerintah hanya menjejalkan edukasi prosedural yang usang, seperti imbauan "jangan asal klik" atau perintah memblokir nomor. Literasi digital masa kini harus berevolusi dengan memasukkan pendekatan berbasis wawasan perilaku (*behavioral insights*). Edukasi seperti ini perlu menyentuh masyarakat akar rumput agar mereka lebih lihai mengendus taktik manipulasi bahasa sekaligus membangun ketahanan emosional. Hasilnya, masyarakat tidak akan mudah panik atau terjebak dalam cara berpikir instan (heuristik) saat menghadapi gempuran pesan intimidasi bermodus kedaruratan palsu di ruang siber.

E. DAFTAR PUSTAKA

Berger, P. L., & Luckmann, T. (1966). *The social construction of reality: A treatise in the sociology of knowledge*. Anchor Books.

Dave. (2025). Manipulative communication in cybercrime: How linguistic tactics deceive digital users. *Journal of Digital Pathology and Communication*, *12*(3), 45–62.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Katz, J. E., & Aakhus, M. (Eds.). (2002). *Perpetual contact: Mobile communication, private talk, public performance*. Cambridge University Press.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Research Consortium on Cyberpsychology. (2023). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *International Journal of Information Security & Psychology*, *8*(1), 112–135.