

**Analisis Modus Operandi Pelaku Pinjaman Online Ilegal dalam Penyalahgunaan Data Digital Ditinjau dari *Fraud Triangle Theory (Opportunity dan Rationalization)***

**Nelly Budiarty, Muhammad Zaky**

Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: nellybudiarty26@gmail.com\*

| <b>Keywords:</b>                                                                                                 | <b>Abstract</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Illegal Online Lending, Modus Operandi, Personal Data Abuse, Fraud Triangle Theory, Cybercrime.</i>           | <i>The proliferation of illegal online lending (pinjol) in Indonesia has escalated cybercrimes involving personal data abuse. Applying the Fraud Triangle Theory, this study analyzes the modus operandi of digital data exploitation. Using a qualitative descriptive approach, primary data were gathered through in-depth interviews with victims, former internal operational employees (desk collection and analysts), and investigators from the South Jakarta Metropolitan Police. The findings reveal that perpetrators manipulate application permissions to access sensitive data (contacts, galleries, and locations) for coercive intimidation. From the opportunity perspective, syndicates utilize upstream data leakages, anonymous VPNs, illegal SIM cards, and dummy bank accounts to maintain digital anonymity. From the rationalization perspective, they justify extreme collection methods as consequences of borrowers' defaults. Concurrently, a counter-rationalization emerges within the "Gagal Bayar" (Galbay) community, where users intentionally defraud the system as resistance. Law enforcement is severely hindered by complex digital anonymity and slow inter-institutional bureaucratic coordination. Thus, strengthening biometric SIM card validation, reinforcing national database security, and streamlining cross-sectoral data integration are vital structural solutions.</i> |
| <b>Kata Kunci:</b>                                                                                               | <b>Abstrak</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Pinjaman Online Ilegal, Modus Operandi; Penyalahgunaan Data Pribadi, Teori Segitiga Kecurangan, Kejahatan Siber. | Maraknya pinjaman online (pinjol) ilegal di Indonesia memicu eskalasi kejahatan siber berupa penyalahgunaan data pribadi. Menggunakan <i>Fraud Triangle Theory</i> , penelitian ini menganalisis modus operandi eksploitasi data digital tersebut. Melalui pendekatan kualitatif deskriptif, data primer dihimpun dari wawancara mendalam bersama korban, mantan karyawan operasional ( <i>desk collection</i> dan analis), serta penyidik Unit Reskrimsus Polres Metro Jakarta Selatan. Hasil kajian mengungkap bahwa pelaku memanipulasi izin akses aplikasi untuk menguasai data sensitif (kontak, galeri, dan lokasi) sebagai instrumen intimidasi. Dari segi peluang ( <i>opportunity</i> ), sindikat memanfaatkan celah kebocoran data hulu, VPN anonim, kartu SIM ilegal, dan rekening fiktif demi menjaga anonimitas digital. Dari segi rasionalisasi, pelaku membenarkan penagihan ekstrem sebagai konsekuensi wanprestasi nasabah. Menariknya, muncul rasionalisasi tandingan dari komunitas "Gagal Bayar" (Galbay) yang sengaja mencurangi sistem sebagai bentuk perlawanan. Penegakan hukum terhambat oleh labirin anonimitas digital pelaku dan lambatnya koordinasi birokrasi antar-lembaga. Oleh karena itu, penguatan validasi biometrik kartu SIM, pengamanan basis data nasional, serta debirokrasi integrasi data lintas sektoral menjadi solusi struktural yang mendesak.                               |

## PENDAHULUAN

Perkembangan teknologi informasi telah melahirkan berbagai inovasi di sektor keuangan, salah satunya *financial technology* (fintech) melalui layanan *peer-to-peer* (P2P) lending (Adji et al., 2023; Purwanto et al., 2022; Sakbaniah et al., 2026). Layanan ini menawarkan kemudahan akses pembiayaan bagi masyarakat yang belum terjangkau layanan perbankan (Wijayanto et al., 2020). Namun, maraknya pinjaman online ilegal menimbulkan berbagai permasalahan, seperti penyalahgunaan data pribadi, penagihan yang tidak etis, dan ancaman terhadap peminjam. Oleh karena itu, diperlukan pengawasan dan regulasi yang efektif untuk melindungi hak-hak konsumen dalam ekosistem keuangan digital. Menurut (Diputra & Ningrum, 2022) *FinTech Lending* merupakan model bisnis keuangan berbasis digital yang memudahkan konsumen untuk mendapatkan pembiayaan atau pinjaman. Fintech Industri keuangan dan investasi mencakup *peer-to-peer fintech lending*, *crowdfunding*, *supply chain finance*, dan lainnya. Industri pembayaran mencakup perbankan seluler, dompet seluler dan online, serta pembayaran *e-commerce* (Dewi, 2026; Hidayatullah, 2025; Idayanti & Ulandari, 2023; Perkasa, 2024).

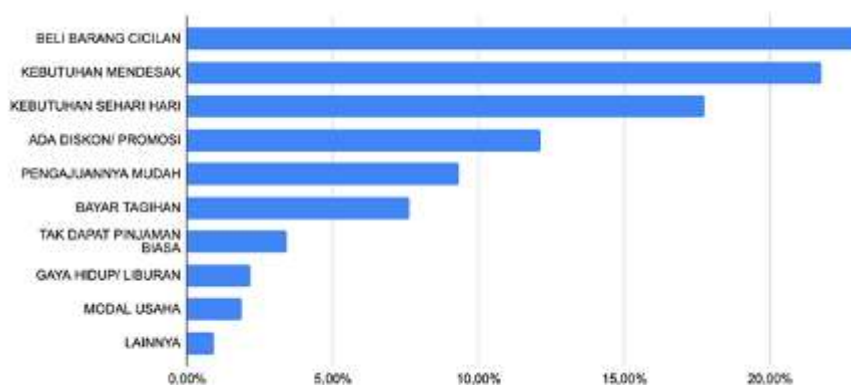
Di balik kemudahan yang ditawarkan layanan *financial technology* (fintech), terdapat persoalan serius terkait penyalahgunaan data pribadi oleh penyelenggara pinjaman online ilegal. Aplikasi pinjaman daring sering meminta akses berlebihan terhadap data pengguna, seperti daftar kontak, galeri foto, dan lokasi, yang kemudian digunakan untuk melakukan intimidasi, ancaman, maupun penyebaran data pribadi guna menekan debitur (Diputra & Ningrum, 2022). Analisis terhadap sejumlah aplikasi fintech juga menunjukkan adanya izin akses (*permissions*) yang tidak relevan dengan fungsi utama aplikasi, sehingga membuka peluang terjadinya penyalahgunaan data pengguna (Wijayanto et al., 2020). Untuk memberikan perlindungan hukum terhadap data pribadi, pemerintah telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur pengumpulan, pemrosesan, dan penyimpanan data pribadi serta memberikan sanksi bagi pelanggar (Undang-Undang Nomor 27 Tahun 2022). Namun demikian, meskipun regulasi tersebut telah berlaku, praktik penyalahgunaan data pribadi oleh pinjaman online ilegal masih terus ditemukan, sehingga diperlukan kajian lebih lanjut mengenai modus operandi pelaku dalam melakukan kejahatan tersebut.

Maraknya praktik pinjaman online ilegal di Indonesia terlihat dari terungkapnya operasi puluhan aplikasi pinjol ilegal yang dijalankan secara terorganisir di Jakarta Utara (Al-Barack, 2025; Tampubolon, 2024; Una, 2026). Kasus tersebut menunjukkan bahwa penyalahgunaan data digital tidak hanya dilakukan secara sistematis, tetapi juga disertai praktik penagihan yang melanggar hukum, seperti ancaman dan penyebaran informasi pribadi korban (ANTARA News, 2021). Pengungkapan dua aplikasi pinjaman online ilegal oleh Bareskrim Polri menunjukkan bahwa praktik penyalahgunaan data pribadi masih menjadi modus utama dalam kejahatan pinjol ilegal. Para pelaku melakukan pemerasan, ancaman, dan penyebaran data pribadi terhadap ratusan korban untuk memaksa pembayaran berulang, bahkan setelah utang dilunasi. Kasus ini menunjukkan bahwa data digital dimanfaatkan sebagai alat kontrol dan eksploitasi terhadap korban (Kepolisian Negara Republik Indonesia, 2025).

Beberapa penelitian telah mengkaji berbagai aspek terkait pinjaman online ilegal dan penyalahgunaan data pribadi di Indonesia, memberikan konteks penting untuk memahami kompleksitas permasalahan ini. Wijayanto et al. (2020) menemukan bahwa aplikasi pinjol ilegal secara sistematis meminta izin akses berlebihan yang dimanfaatkan

untuk penagihan, sementara Diputra dan Ningrum (2022) menyoroti praktik penagihan intimidatif dan perlindungan konsumen yang lemah dalam ekosistem pinjol ilegal. Hidayah (2022) mengungkap bahwa mahasiswa sering menjadi target pinjol ilegal karena rendahnya literasi keuangan dan tekanan ekonomi yang berujung pada teror digital, sedangkan Christian et al. (2024) dan Kaswoto et al. (2025) menganalisis motivasi fraud menggunakan Fraud Triangle Theory, menemukan bahwa tekanan ekonomi, kesempatan akibat lemahnya pengawasan, dan rasionalisasi pelaku merupakan tiga faktor utama pendorong kecurangan. Penelitian tentang penegakan hukum oleh Kepolisian Negara Republik Indonesia (2025) dan Rassat et al. (2022) mendokumentasikan pengungkapan kasus pinjol ilegal yang melibatkan ratusan korban, menunjukkan bahwa modus pemerasan dan ancaman berbasis data digital masih menjadi tantangan utama, serta menyoroti keterorganisasian sindikat dan sulitnya pelacakan pelaku.

Meskipun berbagai penelitian tentang pinjaman online ilegal telah dilakukan, masih terdapat kesenjangan dalam analisis mendalam mengenai modus operandi pelaku dari perspektif teknis-operasional, rasionalisasi pelaku berdasarkan pengakuan internal, fenomena gerakan "Gagal Bayar" (Galbay) sebagai bentuk perlawanan korban, hambatan teknis dan birokrasi kepolisian, serta integrasi Fraud Triangle Theory dari sisi pelaku dan korban secara simultan. Penelitian ini menawarkan kebaruan sebagai studi pertama yang mengkaji modus operandi penyalahgunaan data digital dari tiga sudut pandang (korban, mantan karyawan internal, dan penyidik), mengungkap mekanisme rasionalisasi pelaku berdasarkan data primer, menemukan fenomena "counter-rationalization" dari komunitas Galbay, mengidentifikasi hambatan penegakan hukum termasuk persetujuan digital sebagai tameng pelaku, serta menerapkan Fraud Triangle Theory secara holistik pada pelaku dan korban yang bertransformasi menjadi pelaku.



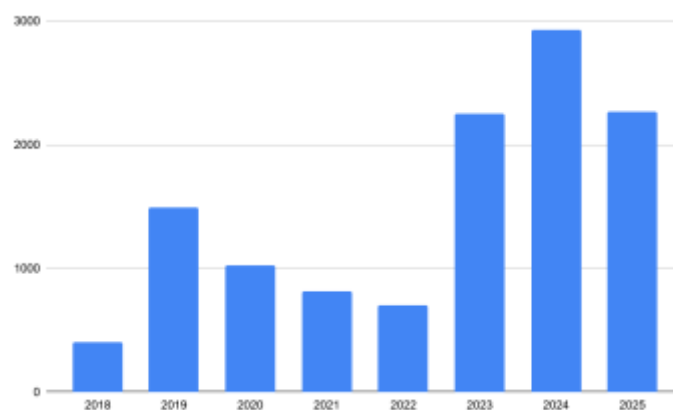
**Gambar 1.** *Data Alasan Masyarakat Indonesia Menggunakan Pinjaman Online/Pinjol (2025)*

*Sumber: Data APJII diolah ulang oleh penulis*

Berdasarkan data yang dihimpun oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2025), penggunaan layanan pinjaman online di Indonesia pada tahun 2025 didominasi oleh kebutuhan yang bersifat konsumtif dan mendesak. Mayoritas masyarakat memanfaatkan pinjaman online untuk membeli barang secara cicilan (23,20%), memenuhi kebutuhan mendesak (21,77%), serta kebutuhan sehari-hari (17,73%). Selain itu, faktor lain seperti adanya promosi atau diskon (12,13%) serta kemudahan dalam proses pengajuan (9,33%) juga menjadi pendorong signifikan. Data

ini menunjukkan bahwa pinjaman online lebih banyak digunakan sebagai solusi praktis untuk memenuhi kebutuhan jangka pendek dibandingkan sebagai sarana pendanaan produktif seperti modal usaha yang persentasenya relatif kecil (1,87%).

Dominasi penggunaan untuk kebutuhan konsumtif dan kondisi darurat tersebut mencerminkan adanya kerentanan ekonomi serta keterbatasan literasi keuangan di kalangan masyarakat. Dalam situasi ini, pengguna cenderung mengutamakan kemudahan dan kecepatan akses tanpa mempertimbangkan secara menyeluruh risiko yang mungkin timbul, khususnya terkait keamanan data pribadi. Proses pengajuan yang sederhana, minimnya verifikasi, serta strategi promosi yang agresif mendorong masyarakat untuk memberikan akses terhadap data digital secara luas tanpa pemahaman yang memadai mengenai konsekuensinya. Kondisi ini pada akhirnya menciptakan peluang (*opportunity*) bagi pelaku pinjaman online ilegal untuk memanfaatkan kelemahan tersebut. Di sisi lain, pelaku juga melakukan rasionalisasi (*rationalization*) dengan menganggap bahwa akses terhadap data pribadi merupakan bagian yang sah dari mekanisme operasional dan penagihan. Akibatnya, penyalahgunaan data digital kerap dijadikan instrumen utama dalam praktik penagihan yang bersifat intimidatif dan berpotensi melanggar hak privasi pengguna.



**Gambar 2.** *Jumlah Entitas Pinjol Ilegal di Indonesia yang Diblokir OJK (2017-2025)*  
*Sumber: OJK Diolah Kembali oleh penulis*

Berdasarkan data dari Otoritas Jasa Keuangan (Otoritas Jasa Keuangan 2025), Pinjaman online ilegal yang diblokir menunjukkan Perkembangan yang dinamis dalam beberapa tahun terakhir, yakni sebanyak 404 entitas pada tahun 2018, meningkat menjadi 1.493 pada tahun 2019, kemudian menurun pada tahun 2020 hingga 2022 masing-masing sebesar 1.026, 811, dan 698 entitas. Namun, pada tahun 2023 dan 2024 terjadi lonjakan signifikan menjadi 2.248 dan 2.930 entitas, sebelum kembali berada pada angka 2.263 entitas pada tahun 2025. Data Otoritas Jasa Keuangan (OJK) menunjukkan bahwa praktik pinjaman online ilegal masih menjadi permasalahan yang serius di Indonesia. Meskipun berbagai upaya penindakan telah dilakukan, jumlah entitas pinjaman online ilegal yang diblokir tetap menunjukkan angka yang tinggi dan cenderung fluktuatif. Sepanjang periode 1 Januari hingga 31 Desember 2025, Otoritas Jasa Keuangan menerima sebanyak 536.267 permintaan layanan melalui Aplikasi Portal Perlindungan Konsumen (APPK), termasuk di dalamnya 56.620 pengaduan. Dari jumlah tersebut, sebanyak 26.220 pengaduan berkaitan dengan aktivitas keuangan ilegal, yang terdiri atas 21.249 pengaduan pinjaman online ilegal dan 4.971 pengaduan investasi ilegal. Jika

dibandingkan dengan jumlah entitas pinjaman online ilegal yang diblokir pada tahun yang sama, terlihat adanya kesenjangan yang cukup signifikan, di mana jumlah pengaduan pinjaman online ilegal hampir sembilan kali lipat lebih besar dibandingkan jumlah entitas yang ditindak.

Penelitian ini bertujuan untuk menganalisis modus operandi pelaku pinjaman online ilegal dalam penyalahgunaan data digital, mengidentifikasi faktor peluang (*opportunity*) yang memungkinkan terjadinya kejahatan siber tersebut, serta mengungkap mekanisme rasionalisasi (*rationalization*) yang digunakan pelaku untuk membenarkan tindakannya. Secara teoritis, penelitian ini diharapkan dapat memperkaya kajian kriminologi siber dan pengembangan Fraud Triangle Theory dalam konteks kejahatan digital di Indonesia. Secara praktis, penelitian ini memberikan rekomendasi bagi aparat penegak hukum, regulator, dan masyarakat dalam upaya pencegahan dan penanganan kejahatan penyalahgunaan data pribadi oleh pinjaman online ilegal.

## **METODE**

Penelitian ini menggunakan pendekatan kualitatif dan jenis penelitian deskriptif karena fokus penelitian adalah mengungkap fenomena penyalahgunaan data pribadi dalam bisnis *fintech lending* ilegal secara menyeluruh dan menyeluruh. Pilihan pendekatan kualitatif didasarkan pada keinginan penelitian untuk memahami proses, konteks, dan makna tindakan pelaku dan pengalaman korban daripada mengukur fenomena secara statistik. Penelitian kualitatif deskriptif menekankan mengamati fenomena sebagaimana adanya melalui analisis dokumen, regulasi, berita, dan kasus aktual. (Snyder, 2019) menyatakan bahwa penelitian kualitatif cocok untuk subjek yang membutuhkan pemahaman interpretatif tentang fenomena sosial berbasis dokumen. Ini terutama berlaku untuk masalah yang berkembang secara dinamis seperti kejahatan digital. (Miles et al., 2014, ) mendukung ini dengan mengatakan bahwa penelitian kualitatif memungkinkan peneliti untuk mempelajari pola, proses dari suatu fenomena. Penelitian deskriptif dirancang untuk memberikan gambaran sistematis, faktual, dan terstruktur tentang cara fintech ilegal menyalahgunakan data pribadi, jenis ancaman digital, dan tindakan regulasi yang tersedia. Dengan demikian, metode ini memungkinkan peneliti mengkaji fenomena secara menyeluruh tanpa mengubah variabel dan menghasilkan pemahaman yang mendalam tentang kekuatan regulasi seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam memberikan perlindungan hukum bagi konsumen yang menjadi korban fintech ilegal.

Teknik pengumpulan data dalam penelitian ini dilakukan melalui wawancara tertutup dan studi kepustakaan. Wawancara tertutup digunakan sebagai teknik pengumpulan data primer dengan menyusun daftar pertanyaan secara terstruktur dan sistematis sesuai dengan fokus penelitian. Analisis data dilakukan melalui tiga tahap secara simultan dan interaktif: reduksi data dengan merangkum dan memfokuskan data relevan dari wawancara dan dokumen; penyajian data dalam bentuk narasi, tabel profil informan, dan matriks tematik; serta penarikan kesimpulan dan verifikasi melalui triangulasi sumber data (korban, pelaku, dan penegak hukum) untuk memastikan keabsahan temuan.

## **HASIL DAN PEMBAHASAN**

Bank Indonesia mengidentifikasi fintech sebagai hasil penyatuan dua elemen (keuangan dan teknologi) sehingga dapat mengubah bentuk bisnis yang tradisional menjadi moderat. Sehingga dahulu transaksi di zaman dahulu dilakukan dengan cara

harus bertatap muka (uang tunai), saat ini transaksi dilakukan dengan metode jarak jauh (Hidayah, 2022).

### ***Profil Informan Penelitian***

Untuk memahami konteks sosial dan operasional dari fenomena penyalahgunaan data pribadi pada pinjaman online (pinjol) ilegal, berikut adalah tabel ringkasan profil informan yang telah dihimpun oleh peneliti:

**Tabel 1.** Profil Informan Penelitian

| <b>Nama/ Inisial</b> | <b>Usia</b> | <b>Peran/Jabatan</b>                                                                                  | <b>Lokasi &amp; Waktu wawancara</b>    |
|----------------------|-------------|-------------------------------------------------------------------------------------------------------|----------------------------------------|
| Putri                | 22 Tahun    | Korban Pinjol Ilegal (Siklus 9 Aplikasi) Wilayah DKI Jakarta                                          | Kedoya, Jakarta Barat; 3 Mei 2026      |
| Adam                 | 23 Tahun    | <i>Complain Analyst</i> (Mantan Kolektor Aplikasi “Koin Semangka”) Wilayah Gading Serpong, Tangerang. | Bintaro, Tangerang Selatan; 6 Mei 2026 |
| Nikol                | 37 Tahun    | <i>Desk Collection</i> Aplikasi “Sinar Rupiah” Wilayah Pluit, Jakarta Utara.                          | Matraman, Jakarta Timur; 14 Mei 2026   |
| Ncak                 | 27 Tahun    | <i>Desk Collection</i> Aplikasi “Sinar Rupiah” Wilayah Pluit, Jakarta Utara.                          | Matraman, Jakarta Timur; 14 Mei 2026   |
| Andhika Prabowo      | -           | Penyidik Unit Reskrimsus                                                                              | Polres Jakarta Selatan; 14 Mei 2026    |

Sumber: Data primer diolah oleh penulis (2026)

### ***Latar Belakang Alasan Keterlibatan dan Struktur Organisasi Internal***

Motivasi di balik keterlibatan individu untuk bekerja di dalam ekosistem pinjaman online (pinjol) ilegal nyatanya dipengaruhi oleh kombinasi faktor desakan ekonomi dan akumulasi pengalaman kerja informal sebelumnya. Berdasarkan data lapangan yang diperoleh dari keterlibatan Informan 2 (Adam) murni didorong oleh motif finansial dan pencarian kompensasi kerja yang lebih kompetitif. Setelah sebelumnya terjebak dalam sistem kerja magang dengan upah minim dan jam kerja yang eksploitatif di sektor retail, Adam memilih beralih ke vendor pihak ketiga pinjol ilegal karena tergiur oleh tawaran kerabatnya. Berdasarkan pengakuannya:

“...Faktor penghasilan, iya. Tapi nomor satu tuh lebih santai... benefitnya jelas.

Kayak mulai dari asuransi BPJS tiap tahun kita ada kerjaan, kompensasi setiap perpanjangan kontrak, THR, kalau misalnya ada kurang gaji juga jelas.”

Fenomena ini menunjukkan bahwa penyedia platform ilegal memanfaatkan celah kerentanan pekerja muda dengan menawarkan paket remunerasi, jaminan sosial (BPJS), dan regulasi waktu kerja yang tampak lebih menjanjikan daripada sektor informal legal. Kondisi yang berbeda ditemukan pada Informan 3 (Nikol), di mana keterlibatannya lebih dipengaruhi oleh modal pengalaman kerja masa lalu dan pengaruh lingkungan sosial. Sebelum beralih ke industri pinjol ilegal, Nikol memiliki rekam jejak kerja di sektor perhotelan yang kemudian bergeser menjadi kolektor lapangan (*debt collector*). Pengalaman koersif di lapangan inilah yang menjadi modal adaptasi bagi Nikol saat ditawarkan masuk ke dalam struktur operasional penagihan digital (*desk collection*) pada platform pinjol ilegal. Realitas ini menegaskan bahwa rekrutmen internal pinjol

ilegal tidak hanya mengandalkan aspek keputusan ekonomi, melainkan juga secara aktif menyerap tenaga kerja terampil yang memiliki spesialisasi dalam bidang penagihan utang.

### ***Mekanisme Eksploitasi Data Pribadi Nasabah melalui Celah Digital***

pintu masuk utama kebocoran data bermula dari kelalaian nasabah yang menyetujui klausul perjanjian panjang tanpa membaca secara saksama saat instalasi aplikasi. Namun, pada tahap operasional, tekanan pemenuhan target penagihan memicu karyawan bertindak melampaui Prosedur. Lebih jauh lagi, sindikat pinjol ilegal memiliki instrumen penetrasi siber terstruktur guna mengantisipasi nasabah yang memutuskan komunikasi atau mematikan ponsel. Para pelaku memanfaatkan aplikasi pihak ketiga seperti *Get Contact* untuk melacak lokasi kerja, serta melakukan pemindaian media sosial (*Instagram dan LinkedIn*) guna mendeteksi jaringan pertemanan dan profesi korban. Guna membongkar privasi kependudukan nasabah secara radikal, pelaku juga mengintegrasikan alat siber ilegal berupa bot Telegram bernama "Edamu". Temuan ini menegaskan bahwa kejahatan siber pinjol ilegal tidak lagi sekadar mengandalkan data statis yang didaftarkan nasabah, melainkan telah berkembang menggunakan instrumen pelacakan digital yang masif untuk melanggar privasi korban secara agresif.

### ***Modus Intimidasi Psikologis, Penyuntingan Foto, dan Rekayasa Sosial dalam Penagihan***

Fase setelah penguasaan data pribadi dilanjutkan dengan pemetaan terhadap titik lemah atau ketakutan terbesar korban guna meluncurkan teror psikologis yang spesifik. Informan 4 (Ncak) memaparkan bahwa salah satu taktik paling destruktif yang dilakukan oleh *desk collection* adalah ancaman penyebaran foto orisinal dari galeri ponsel nasabah yang telah dimanipulasi secara asusila dengan tujuan memberikan efek jera, mempermalukan, serta meruntuhkan kondisi mental korban di hadapan lingkaran keluarga maupun lingkungan kerja. Tekanan sosiologis ini memaksa korban berada dalam kondisi panik sehingga bersedia melakukan segala cara untuk melunasi utang, termasuk terjebak ke dalam siklus *gali lubang tutup lubang*.

Selain manipulasi visual, sindikat pinjol ilegal juga menerapkan metode rekayasa sosial yang sangat manipulatif untuk men teror korban di dunia nyata:

1. **Manipulasi Lokasi (*Screenshot Google Maps Palsu*):** Pelaku mengambil foto rumah nasabah melalui fitur *Google Street View* dan mengirimkannya kepada korban untuk menciptakan ilusi psikologis seolah-olah penagih lapangan (*debt collector*) telah mengepung kediaman mereka.
2. **Adu Domba Kontak (*Social Pressuring*):** Pelaku mengirimkan pesan acak ke nomor rekan atau keluarga korban dengan narasi fitnah bahwa pemilik kontak tersebut ikut menikmati uang pinjaman. Taktik adu domba ini bertujuan agar lingkungan sosial ikut memberikan tekanan secara langsung kepada korban.

### ***Modus Operandi Kejahatan Siber Lanjutan dan Dampak Viktimisasi Psikologis***

Ketika korban memasuki fase tidak mampu membayar (gagal bayar), platform pinjaman online ilegal mengeskalisasi tindakannya melalui pencurian identitas (*identity theft*) dan pencemaran nama baik secara masif. Data kontak dan galeri ponsel yang telah disalin sebelumnya diaktifkan sebagai instrumen teror. jaringan sindikat ini juga meluncurkan kejahatan siber lanjutan berupa *phishing*. Pelaku mengirimkan tautan (*link*) manipulatif dengan dalih "prosedur cara pembayaran baru" yang dirancang untuk meretas sistem dan menguras isi saldo *mobile banking* korban secara otomatis.

### ***Kendala "Persetujuan Digital" (*Application Permission*) Sebagai Tameng Hukum***

salah satu titik krusial yang menyulitkan penindakan instan adalah adanya klausul persetujuan digital (*application permission*) di fase awal instalasi aplikasi. Kelalaian

konsumen yang langsung menyetujui hak akses nomor telepon dan foto secara tidak sengaja memberikan legalitas siber awal bagi sistem pelaku untuk menduplikasi data pribadi mereka. Adanya unsur persetujuan (*consent*) ini mempersulit penyidik kepolisian untuk menjerat pelaku dengan pasal pencurian data murni. Di samping dilema konstruksi hukum tersebut, Unit Reskrimsus juga membentur hambatan teknis tingkat tinggi dalam proses pengumpulan alat bukti digital untuk melacak pelaku. Jaringan sindikat pinjol ilegal secara terorganisir mengaburkan jejak operasional mereka melalui teknik pengacakan Alamat Protokol Internet (*IP Address*) dengan mengeksploitasi teknologi *Virtual Private Network* (VPN) dan (*server*) proksi yang terus berubah.

### ***Hambatan Birokrasi dan Koordinasi Lintas Instansi***

Proses pelacakan aliran dana dan pembekuan rekening penampung milik sindikat pelaku tidak dapat dieksekusi secara mandiri oleh penyidik kepolisian. Kepolisian harus melewati mekanisme administrasi formal yang berlapis, di mana permohonan data harus diajukan ke Otoritas Jasa Keuangan (OJK) terlebih dahulu sebelum diteruskan ke pihak perbankan. Ketatnya proteksi internal lembaga perbankan terhadap data nasabah sering kali memperlambat pengumpulan bukti finansial digital. Kelambatan penanganan yang disebabkan oleh birokrasi surat-menyurat ini secara tidak langsung memberikan celah waktu bagi pelaku. Selain hambatan prosedural di atas, penegakan hukum siber juga terkendala oleh lemahnya arsitektur hukum nasional. Pihak kepolisian memberikan kritik fundamental terhadap regulasi keamanan siber dan perlindungan data kependudukan di Indonesia yang ada saat ini. Instrumen perundang-undangan perlindungan data dinilai masih sangat lemah dan implementasinya jauh dari kata maksimal. Ketiadaan perlindungan siber yang agresif dan komprehensif ini memicu kerentanan besar, di mana data pribadi warga negara terkesan dibiarkan diakses secara bebas tanpa batas wilayah. Kondisi ini menegaskan perlunya reformasi hukum yang berfokus pada debirokrasi koordinasi penegakan hukum siber serta penguatan regulasi demi menjaga kedaulatan digital nasional.

penyidik kepolisian menyoroti bahwa instrumen undang-undang perlindungan data yang ada saat ini belum mampu memberikan proteksi maksimal. Lemahnya sistem pengamanan membuat data kependudukan nasional terkesan bersifat terbuka (*open source*) sehingga dapat diakses secara bebas tanpa batas wilayah perlindungan kedaulatan digital, bahkan hingga ke luar negeri. Kondisi pengawasan yang minim dari dalam negeri ini secara tidak langsung memberikan kelonggaran siber yang menguntungkan sindikat kriminal internasional dalam mengeksploitasi identitas warga negara.

### ***Perangkap Konsep Coerced Consent (Persetujuan Digital yang Dimanipulasi)***

Secara yuridis, Pasal 19 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi secara eksplisit mengamanatkan bahwa Proses data pribadi wajib berlandaskan pada persetujuan yang sah secara hukum dan diberikan secara eksplisit untuk tujuan yang spesifik. Namun, dalam ekosistem pinjol ilegal, sindikat pelaku secara sengaja menyembunyikan hak menduplikasi isi galeri, melacak daftar kontak, hingga penyebaran data di balik lembar Syarat dan Ketentuan (*terms and conditions*) yang sengaja dibuat sangat panjang. Kondisi sosiologis masyarakat yang memiliki literasi digital rendah, ditambah tekanan psikologis akibat desakan finansial instan, membuat nasabah cenderung langsung menekan tombol "*Izinkan Akses*" tanpa meneliti implikasi hukumnya. Konsekuensinya, tindakan asal klik tersebut secara ironis bertransformasi menjadi "tameng legalitas" bagi pelaku ketika dihadapkan pada hukum formal.

### ***Analisis Opportunity dalam Fraud Triangle Theory***

Dalam teori Fraud Triangle, yaitu peluang (*opportunity*), merupakan faktor yang menjelaskan bagaimana situasi atau kondisi tertentu memberi kesempatan bagi individu untuk melakukan kecurangan atau penipuan. Dalam konteks Fraud Triangle Theory, peluang muncul ketika individu merasa ada kesempatan untuk melakukan kecurangan tanpa terdeteksi, yang bisa timbul dari lemahnya pengendalian internal, kebijakan yang kurang ketat, atau kurangnya pengawasan (Kaswoto et al., 2025). Dalam kerangka Fraud Triangle Theory yang dicetuskan oleh Donald R. Cressey, dimensi *opportunity* (kesempatan) menempati posisi krusial sebagai pemicu eksternal yang memungkinkan suatu tindak kejahatan dapat terlaksana. Berbeda dengan motif internal pelaku, kesempatan ini lahir dari kelemahan sistem digital, kelonggaran pengawasan, celah regulasi, serta rendahnya literasi digital masyarakat yang kemudian dieksploitasi oleh sindikat pinjaman online ilegal dalam menyalahgunakan data pribadi pengguna. Kesempatan muncul ketika terdapat kelemahan dalam sistem pengawasan, regulasi, atau mekanisme kontrol yang dapat dimanfaatkan oleh pelaku untuk menjalankan tindakannya. Dalam konteks kejahatan modern, *opportunity* sering kali berkaitan erat dengan perkembangan teknologi dan kompleksitas sistem digital yang sulit diawasi secara menyeluruh. Untuk ini manifestasi peluang ini terbagi ke dalam dua aspek utama:

#### **1. Persetujuan Akses Aplikasi yang Bersifat Manipulatif:**

Kesempatan kriminal muncul sejak fase awal pengunduhan, di mana aplikasi meminta otoritas akses terhadap kontak, galeri, kamera, dan lokasi korban. Desakan kebutuhan finansial yang cepat memaksa korban langsung memberikan persetujuan tanpa meneliti Syarat dan Ketentuan secara rinci. Padahal, tindakan menyisipkan izin akses data secara tersembunyi ini bertentangan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengamanatkan kejelasan tujuan penggunaan data. Kondisi persetujuan digital ini pun kerap menjadi tameng sekaligus kendala bagi kepolisian dalam menjerat pelaku di tingkat penegakan hukum formal.

#### **2. Mudahnya Akses terhadap Data Digital dan Alat Pelacakan Siber**

Peluang ini diperlebar oleh masih rapuhnya proteksi ekosistem data digital di Indonesia. Lemahnya perlindungan ini dimanfaatkan pelaku untuk menghimpun data tambahan korban secara ilegal melalui berbagai instrumen pelacakan siber luar yang marak beredar bebas di internet, seperti penggunaan fitur bot otomatis di platform Telegram. Melalui alat pelacak tersebut, pelaku dapat dengan mudah membongkar privasi korban guna mengeskalisasi intensitas penagihan.

### ***Analisis Faktor Rasionalisasi (Rationalization) Pelaku dalam Kejahatan Siber***

Berdasarkan *Fraud Triangle Theory* yang dirumuskan oleh Donald R. Cressey, rasionalisasi merupakan elemen psikologis-kognitif internal yang terjadi di dalam personalitas pelaku sebelum atau saat melakukan tindakan kejahatan. Berbeda dengan aspek eksternal seperti kesempatan (*opportunity*), rasionalisasi berfungsi sebagai mekanisme pertahanan diri berupa pembenaran moral internal. Mekanisme ini memungkinkan sindikat pinjaman online ilegal untuk menjalankan kejahatan siber tanpa harus merasa bersalah atau menganggap dirinya melanggar hukum, dengan cara mengaburkan sifat melawan hukum menjadi sesuatu yang dianggap wajar secara situasional. Menurut (Christian et al., 2024) Rasionalisasi bisa terjadi dalam berbagai situasi, termasuk di lingkungan kerja dimana tekanan untuk mencapai target atau memenuhi ekspektasi bisa memicu perilaku tidak jujur. *Rationalization* juga berkaitan dengan persepsi pelaku terhadap anonimitas dan jarak sosial dalam ruang digital. Interaksi yang tidak bersifat tatap muka cenderung mengurangi empati pelaku terhadap

korban, sehingga tindakan penyalahgunaan data dipandang sebagai aktivitas yang tidak menimbulkan dampak nyata.

Berdasarkan hasil wawancara mendalam terhadap karyawan (*desk collection*), penulis mengkategorikan tiga bentuk rasionalisasi siber dominan yang melandasi penyalahgunaan data pribadi dan pencemaran nama baik digital yaitu:

**1. Doktrin Persetujuan Digital Sukarela sebagai Legitimasinya Pelanggaran Privasi (*Victim Blaming*)**

Pelaku mengadopsi mekanisme *victim blaming* dengan melempar kesalahan sepenuhnya kepada pihak korban. Pelaku merasionalisasikan bahwa tindakan seperti menyalin isi galeri, menarik daftar kontak, hingga menyebarkan rekayasa foto asusila bukanlah kejahatan murni, melainkan konsekuensi transaksional logis yang telah disepakati nasabah secara sukarela sejak awal transaksi.

**2. Rasionalisasi Status Hukum Perikatan yang Ilegal**

Bentuk rasionalisasi kedua bersumber dari kesadaran pelaku bahwa platform mereka beroperasi di luar lingkup hukum formal (tidak terdaftar di OJK). Pelaku memahami bahwa perikatan utang-piutang tersebut secara hukum tidak sah berdasarkan ketentuan Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata) karena objek dan klausul operasionalnya tidak halal. Kesadaran akan ketiadaan perlindungan hukum formal ini justru memicu rasionalisasi siber di fikiran pelaku untuk membenarkan tindakan penyalahgunaan data digital.

**3. Transformasi Korban Menjadi Pelaku Melalui Gerakan Gagal Bayar (Galbay)**

masyarakat yang semula diklasifikasikan sebagai "korban" eksploitasi data pribadi, pada titik tertentu melakukan pergeseran peran secara sadar menjadi pelaku kecurangan ekonomi melalui gerakan Gagal Bayar (Galbay) secara sengaja. Dinamika pembalikan peran dari korban menjadi pelaku ini digerakkan oleh perpaduan komponen kesempatan (*opportunity*) dan rasionalisasi (*rationalization*) dari sisi nasabah. Pemanfaatan Kesempatan (*Opportunity*) oleh Nasabah memanfaatkan celah hukum di mana platform pinjol ilegal tidak memiliki kekuatan hukum perdata untuk menuntut mereka ke pengadilan formal.

Selain itu, masyarakat membentuk Rasionalisasi Kelompok dalam Komunitas Galbay yang menjadi tindakan melarikan uang yang disahkan oleh nasabah melalui mekanisme rasionalisasi kelompok secara massal di media sosial (seperti grup Facebook Komunitas Galbay). Mereka mengonstruksikan narasi moralitas baru bahwa mengambil uang dari platform ilegal secara gratis merupakan bentuk hukuman sosial yang sah atas rusaknya tatanan masyarakat akibat pinjol ilegal.

***Kendala Penanganan Kasus Pinjaman Online Ilegal oleh Unit Kepolisian***

Penyalahgunaan data pribadi oleh kelompok pinjaman online ilegal merupakan tindakan kejahatan siber yang terorganisir dari awal hingga akhir. Pada fase awal, pelaku memanfaatkan rendahnya penguasaan digital dan tekanan keuangan dari korban dengan menggunakan metode manipulatif untuk mendapatkan persetujuan digital agar bisa menggandakan kontak serta galeri di ponsel. Ketika terjadi keterlambatan pembayaran, data ini digunakan untuk tujuan teror koersif melalui cara-cara seperti pencurian identitas visual, pembajakan akun, dan memperburuk hubungan sosial korban melalui provokasi antar kontak. Menariknya, tekanan ini mendorong munculnya fenomena tumpang tindih antara korban dan pelaku, di mana beberapa korban ikut terlibat dalam tindakan penipuan ekonomi dengan secara sengaja melakukan gerakan gagal bayar secara massal dan memanfaatkan dana aplikasi melalui jaringan di media sosial.

Di fase akhir, usaha represif dari Unit Siber Kepolisian dalam menanggulangi jaringan ini dihadapkan pada berbagai rintangan teknis, birokrasi, dan regulasi yang

rumit. Penyelidik di lapangan menemukan kesulitan dalam melacak pelaku utama karena pola anonimitas digital yang digunakan oleh mereka, seperti VPN yang berubah-ubah, kartu SIM palsu, serta transaksi jual-beli rekening bank tidak sah milik masyarakat berpenghasilan rendah. Efektivitas penegakan hukum semakin terhambat oleh panjangnya rantai birokrasi yang melibatkan koordinasi antar lembaga antara Kepolisian, OJK, dan pihak perbankan, yang memberi kesempatan bagi pelaku untuk menghilangkan bukti kejahatan. Oleh karena itu, kepolisian menegaskan bahwa pemberantasan pinjaman online ilegal tidak dapat difokuskan hanya pada tindakan represif di lapangan, melainkan juga memerlukan reformasi struktural dengan memperkuat regulasi perlindungan data nasional yang masih lemah, peningkatan integrasi basis data kependudukan, serta memudahkan akses perbankan secara langsung.

## KESIMPULAN

Hasil penelitian menunjukkan bahwa penyalahgunaan data digital oleh pelaku pinjaman online ilegal dilakukan secara terorganisir melalui pemanfaatan akses data pribadi korban yang diperoleh melalui aplikasi pinjaman. Ditinjau dari aspek *opportunity*, kejahatan ini didukung oleh lemahnya perlindungan data, anonimitas digital, serta penggunaan identitas dan rekening yang sulit dilacak. Sementara itu, dari aspek *rationalization*, pelaku membenarkan tindakan penyalahgunaan data dan penagihan intimidatif sebagai konsekuensi atas kegagalan debitur memenuhi kewajibannya. Penelitian ini juga menemukan adanya fenomena di mana sebagian masyarakat merasionalisasi praktik gagal bayar terhadap pinjol ilegal sebagai bentuk perlawanan, yang kemudian memicu tindakan represif dari pelaku. Temuan ini menunjukkan perlunya penguatan perlindungan data pribadi, peningkatan pengawasan terhadap pinjaman online ilegal, serta optimalisasi koordinasi antarinstansi dalam penegakan hukum kejahatan siber. Berdasarkan temuan tersebut, beberapa saran diajukan. Bagi aparat penegak hukum, diperlukan penguatan koordinasi lintas instansi dan debirokrasi akses data perbankan untuk mempercepat penindakan. Bagi regulator (OJK dan Kominfo), pengawasan terhadap perizinan akses data aplikasi pinjol perlu diperketat dan sanksi bagi pelanggar dipertegas. Bagi masyarakat, peningkatan literasi digital sangat penting agar lebih waspada terhadap izin akses aplikasi dan tidak mudah terjebak dalam jeratan pinjol ilegal. Penelitian selanjutnya disarankan untuk mengkaji efektivitas implementasi UU PDP dalam kasus pinjol ilegal serta melakukan studi perbandingan dengan negara lain.

## REFERENSI

- Adji, Y. B., Muhammad, W. A., Akrabi, A. N. L., & Noerlina, N. (2023). Perkembangan inovasi fintech di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 5(1), 47–58.
- Al-Barack, A. (2025). *Pengawasan otoritas jasa keuangan terhadap aplikasi pinjaman online ilegal: The supervision of the Financial Services Authority over illegal online lending applications*. Universitas Hasanuddin Makassar.
- APJII. (2025, August 8). *Alasan warga RI pakai pinjol, mayoritas untuk beli barang cicilan*. Databoks. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/689565a3e9031/alasan-warga-ri-pakai-pinjol-mayoritas-untuk-beli-barang-cicilan>
- Christian, N., Arlina, A., Tryany, J., & Liang, V. L. (2024). Analisis motivasi fraud dengan pendekatan teori fraud. *Jurnal Sains Manajemen dan Akuntansi*, 16(1), 86.

<https://doi.org/10.37151/jsma.v16i1.173>

- Dewi, R. (2026). *ShopeePay: Sinergi e-commerce dan sistem pembayaran terintegrasi*. Afdan Rojabi Publisher.
- Diputra, & Ningrum. (2022, January 15). Pelanggaran etika bisnis fintech lending ilegal terhadap debitur. *[Nama jurnal tidak dicantumkan]*, 43(1), 63–66.
- Hidayah, A. (2022). Membongkar sisi gelap fintech peer-to-peer lending (pinjaman online) pada mahasiswa di Yogyakarta. *Jurnal Hukum dan Sosial*, 1(1), 2–3. <https://ejournal.upgrisba.ac.id/index.php/jhs/article/view/6189>
- Hidayatullah, A. S. (2025). Analisis nilai manfaat sistem pembayaran cash on delivery saat menggunakan aplikasi dompet digital. *Jurnal Ekonomi Utama*, 4(2), 441–450.
- Idayanti, R., & Ulandari, P. (2023). Peran aplikasi dompet digital Indonesia (DANA) dalam memudahkan masyarakat melakukan pembayaran digital. *Islamic Banking and Finance Journal*, 3(2).
- Kaswoto, J., Budiman, M., Mubarok, A. Z., Sugihyanto, T., Wahyono, Z., & Sudarmanto, E. (2025). Tafsir ekonomi: Pencegahan kecurangan dengan pendekatan teori fraud triangle dalam perspektif Tafsir Jalalain. *Jurnal Ilmiah Ekonomi Islam*, 11(1), 234–236. <https://www.jurnal.stie-aas.ac.id/index.php/jei/article/view/16934>
- Kepolisian Negara Republik Indonesia. (2025, November 21). *Bareskrim Polri bongkar 2 aplikasi pinjol ilegal, 400 korban diperas dan diancam*. <https://humas.polri.go.id/news/detail/2180645-bareskrim-polri-bongkar-2-aplikasi-pinjol-ilegal-400-korban-diperas-dan-diancam>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook*. SAGE Publications.
- Otoritas Jasa Keuangan. (2025). *Siaran pers RDKB Februari 2025: Stabilitas sektor jasa keuangan tetap terjaga di tengah meningkatnya dinamika perekonomian*. Otoritas Jasa Keuangan.
- Perkasa, U. N. (2024). Pengaruh penggunaan dompet digital dan e-commerce terhadap keberlangsungan usaha mikro, kecil dan menengah (Studi literature UMKM). *Jurnal Manajemen, Akuntansi dan Logistik (JUMATI)*, 2(2).
- Purwanto, H., Yandri, D., & Yoga, M. P. (2022). Perkembangan dan dampak financial technology (fintech) terhadap perilaku manajemen keuangan di masyarakat. *Kompleksitas: Jurnal Ilmiah Manajemen, Organisasi dan Bisnis*, 11(1), 80–91.
- Rassat, F. S., Sujatmiko, E., & ANTARA News. (2022, January 26). *Ruko di Pantai Indah Kapuk operasikan 14 aplikasi pinjol ilegal*. ANTARA News. <https://www.antaranews.com/berita/2667153/ruko-di-pantai-indah-kapuk-operasikan-14-aplikasi-pinjol-ilegal>
- Sakbaniah, N., Melviyanti, N., Adha, F. H., & Agustina, Z. (2026). Regulasi dan manajemen risiko layanan fintech peer-to-peer lending di Indonesia: Penelitian pusaka aspek hukum dan perbankan. *Media Hukum Indonesia (MHI)*, 4(3).
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Tampubolon, R. S. H. (2024). *Upaya penegakan hukum pidana oleh kepolisian terhadap tagihan pinjaman online ilegal dengan ancaman terhadap konsumen*. Universitas Medan Area.
- Una, B. K. (2026). *Pinjaman online di Indonesia: Menjembatani keuangan ataukah perangkap digital?* Deepublish.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196*,

*Tambahan Lembaran Negara Republik Indonesia Nomor 6820.*  
<https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>

Wijayanto, H. (2020). Analisis penyalahgunaan data pribadi dalam aplikasi fintech ilegal dengan metode hibrid. *Jurnal Sains dan Informatika*, 18(1), 1.  
<https://doi.org/10.30646/sinus.v18i1.433>