Abdurrauf Science and Society
Vol. 2, No. 2, 2026, pp. 91~102
ISSN: 3090-093X; DOI: 10.70742/asoc.v2i2.532

Pengaruh Media Sosial Terhadap Penyalahgunaan Informasi dan Transaksi Elektronik (ITE) di Kabupaten Sinjai

The Influence of Social Media on the Misuse of Information and Electronic Transactions (ITE) in Sinjai Regency

Riska[1]*, Nirwati Ningsih[2], Nurfaikatunnisa[3] ,Syardayana[4],St.Khadijah wahid[5]
[1-5]Fakultas Ekonomi dan Hukum Islam, Universitas Islam Ahmad Dahlan Sinjai, Indonesia
Email: riska06052005@gmail.com, nirwatiningsih@gmail.com, nurfaikatunnisa5@gmail.com, Syrdyn344@gmail.com, ijha747@gmail.com

ARTICLE INFO

Article history:

Received 10-12-2025
Accepted 22-02-2026
Published 26-02-2026

Keywords:

ITE Crimes
Digital Transactions
kabupaten Sinjai

***Corresponding Author:**

Competing interest:
The author(s) have declared that no competing interests exist

ABSTRACT

The advancement of information technology and electronic transactions in the digital era has provided various conveniences in people's lives. However, at the same time, it has also given rise to different forms of crime in the field of information and electronic transactions. These crimes include online fraud, data theft, identity misuse, and the dissemination of harmful content, all of which result in material losses and a decline in public trust in digital systems. In Sinjai Regency, the practice of electronic transaction crimes has become increasingly evident through the growing number of online fraud cases, as well as the spread of content that violates legal provisions through social media. This study aims to analyze and understand the phenomenon of the misuse of Information and Electronic Transactions (ITE) occurring in Sinjai Regency. The research method employed is library research with a qualitative approach, utilizing secondary data in the form of books, scientific journals, articles, legislation, and other supporting documents. The findings indicate that information and electronic transaction crimes in Sinjai Regency exhibit diverse characteristics and patterns, thereby requiring active involvement from law enforcement authorities as well as improved digital literacy among the public. Therefore, strengthening regulations, enhancing digital education, and establishing effective coordination among relevant stakeholders are necessary to create a safe and trustworthy digital environment.

Citation:
Riska, R., Ningsih, N. ., Nurfaikatunnisa, N., Yana, S. ., & Wahid, S. . (2026). Pengaruh Media Sosial Terhadap Penyalahgunaan Informasi dan Transaksi Elektronik (ITE) di Kabupaten Sinjai . *Abdurrauf Science and Society*, *2*(2), 91–102. https://doi.org/10.70742/asoc.v2i2.532

ABSTRAK

*Kemajuan teknologi informasi dan transaksi elektronik di era digital telah memberikan berbagai kemudahan dalam kehidupan masyarakat, namun pada saat yang sama juga memunculkan berbagai bentuk kejahatan di bidang informasi dan transaksi elektronik. Bentuk kejahatan tersebut antara lain penipuan berbasis daring, pencurian data, penyalahgunaan identitas, serta penyebaran konten negatif yang berdampak pada kerugian secara materiil dan menurunnya tingkat kepercayaan masyarakat terhadap sistem digital. Di Kabupaten Sinjai, praktik kejahatan transaksi elektronik semakin terlihat melalui maraknya kasus penipuan online, serta penyebaran konten yang melanggar ketentuan hukum melalui media sosial. Penelitian ini bertujuan untuk menganalisis dan memahami fenomena penyalahgunaan Informasi dan Transaksi Elektronik (ITE) yang terjadi di Kabupaten Sinjai. Metode penelitian yang digunakan adalah penelitian kepustakaan (*library research*) dengan pendekatan kualitatif, yang memanfaatkan data sekunder berupa buku, jurnal ilmiah, artikel, peraturan perundang-undangan, serta dokumen pendukung lainnya. Hasil kajian menunjukkan bahwa kejahatan informasi dan transaksi elektronik di Kabupaten Sinjai memiliki ciri dan pola yang beragam, sehingga menuntut keterlibatan aktif aparat penegak hukum serta peningkatan literasi digital di kalangan masyarakat. Oleh karena itu, diperlukan penguatan regulasi, peningkatan edukasi digital, serta koordinasi yang efektif antar pihak terkait guna menciptakan ruang digital yang aman dan dapat dipercaya.*

Kata Kunci: *Kejahatan ITE Transaksi Digital kabupaten Sinjai*

PENDAHULUAN

Kejahatan informasi dan transaksi elektronik merupakan salah satu tantangan terbesar diera digital saat ini. Dengan perkembangan teknologi informasi yang sangat pesat, aktivitas manusia semakin banyak bergantung pada sistem elektronik, mulai dari komunikasi, transaksi keuangan, hingga penyimpanan data penting. Namun, kemudahan dan kecepatan yang ditawarkan oleh teknologi juga membuka peluang bagi pelaku kejahatan untuk melakukan tindakan ilegal yang merugikan individu maupun institusi. Hal ini menimbulkan kebutuhan mendesak untuk memahami dan menangani aspek kejahatan yang berkaitan dengan penggunaan teknologi informasi dan transaksi elektronik (Munajat & Yusuf, 2024).

Kejahatan informasi meliputi berbagai tindakan kriminal yang menggunakan teknologi informasi sebagai media atau sasaran, seperti peretasan, pencurian data, penyebaran virus, hingga penyalahgunaan data pribadi. Di sisi lain, kejahatan transaksi elektronik menitikberatkan pada tindak kejahatan yang terjadi dalam proses transaksi digital, termasuk penipuan online, pemalsuan dokumen elektronik, dan manipulasi sistem pembayaran digital. Kedua jenis kejahatan ini memiliki dampak besar, tidak hanya pada kerugian materi tetapi juga pada kepercayaan masyarakat terhadap sistem elektronik yang semakin penting dalam kehidupan sehari-hari (Udayana et al., 2025).

Dalam konteks hukum dan regulasi, upaya penanggulangan kejahatan informasi dan transaksi elektronik menjadi fokus utama pemerintah dan lembaga terkait. Pentingnya perlindungan terhadap data dan transaksi elektronik mendorong munculnya berbagai peraturan dan mekanisme pengawasan yang ketat. Namun, tantangan terbesar tetap pada adaptasi regulasi dengan cepatnya perkembangan teknologi dan strategi pelaku kejahatan yang semakin canggih. Oleh karena itu, pemahaman mendalam tentang karakteristik, modus operandi, serta upaya pencegahan kejahatan di ranah digital menjadi sangat esensial untuk menjaga keamanan dan integritas sistem informasi serta transaksi elektronik (Setiawan, 2024).

Di Kabupaten Sinjai, kasus kejahatan informasi dan transaksi elektronik semakin nyata dengan terungkapnya sejumlah kasus penipuan online yang merugikan masyarakat. Salah satu kasus yang menonjol adalah penipuan dengan modus jual beli hasil bumi, seperti cengkeh, yang menyebabkan kerugian mencapai ratusan juta rupiah. Dalam modus ini, pelaku menggunakan identitas palsu untuk memanipulasi korban dengan skema segitiga,

sehingga korban sampai mengirimkan barang namun tidak menerima pembayaran yang semestinya. Kasus ini mencerminkan bagaimana kejahatan elektronik dapat menyasar aktivitas ekonomi lokal yang sangat bergantung pada sistem transaksi digital.

Penanganan kejahatan transaksi elektronik di Sinjai juga mendapatkan perhatian dari aparat kepolisian yang secara aktif mengungkap dan menangkap para pelaku. Polres Sinjai misalnya, telah melakukan berbagai operasi untuk memberantas penipuan online tersebut, termasuk menyosialisasikan kewaspadaan kepada masyarakat agar tidak mudah tertipu oleh skema kriminal di dunia maya. Kasus-kasus semacam ini menjadi bukti nyata bahwa kejahatan di ranah digital sudah sangat mendekati dan merasakan dampaknya langsung oleh komunitas di tingkat kabupaten.

Selain penipuan, kasus lain yang menjadi perhatian adalah penyebaran konten negatif atau konten yang melanggar hukum melalui media sosial di Sinjai. Fenomena ini juga masuk dalam kategori kejahatan informasi, di mana penyebaran berita palsu, fitnah, atau konten yang melanggar asas hukum dapat merusak reputasi individu atau institusi. Hal ini menambah kompleksitas tantangan keamanan informasi dan transaksi elektronik yang harus dihadapi oleh pemerintah dan masyarakat di Kabupaten Sinjai, sehingga perlindungan hukum dan edukasi digital menjadi sangat penting.

Dengan demikian, kejahatan informasi dan transaksi elektronik di Kabupaten Sinjai tidak hanya terjadi dalam bentuk penipuan finansial secara online tetapi juga mencakup berbagai tindakan ilegal lain yang memanfaatkan kemajuan teknologi digital. Penanganan kasus-kasus tersebut memerlukan koordinasi antara aparat hukum, masyarakat, dan pihak terkait agar tercipta lingkungan digital yang aman dan terpercaya.

METODE

Penelitian ini disusun secara deskriptif dengan menggunakan metode penelitian kepustakaan (library research) dan pendekatan kualitatif. Metode ini dipilih karena penelitian bertujuan untuk mengkaji dan memahami fenomena penyalahgunaan Informasi dan Transaksi Elektronik (ITE) di Kabupaten Sinjai melalui analisis sumber-sumber tertulis yang relevan, sehingga dapat diperoleh gambaran yang sistematis dan komprehensif mengenai permasalahan yang diteliti.Jenis penelitian ini adalah penelitian hukum normatif yang bersifat deskriptif-analitis. Penelitian hukum normatif berfokus pada kajian terhadap norma, asas, dan kaidah hukum yang mengatur penyalahgunaan ITE, khususnya dalam kerangka hukum positif Indonesia. Penelitian ini tidak melakukan pengumpulan data lapangan, melainkan menitikberatkan pada analisis bahan pustaka sebagai sumber utama untuk menjelaskan bentuk, faktor, dan implikasi hukum dari penyalahgunaan ITE di Kabupaten Sinjai.Pendekatan yang digunakan dalam penelitian ini Pendekatan Perundang-undangan (statute approach) , yaitu dengan menelaah peraturan yang berkaitan dengan Informasi dan Transaksi Elektronik, terutama ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, serta regulasi lain yang relevan. Data yang telah dikumpulkan dianalisis menggunakan metode kualitatif deskriptif-analitis, dengan mekanisme Reduksi Data, yaitu menyeleksi dan memfokuskan data yang relevan dengan rumusan masalah penelitian.Klasifikasi Data, yaitu mengelompokkan data berdasarkan kategori tertentu, seperti bentuk penyalahgunaan ITE (penipuan online, pencemaran nama baik, penyebaran konten ilegal), aspek regulasi, dan dampak sosial.Analisis Normatif, yaitu menafsirkan dan mengkaji ketentuan hukum yang berlaku, khususnya dalam UU ITE, untuk melihat kesesuaian antara norma hukum dan fenomena yang terjadi.

HASIL DAN PEMBAHASAN

Pengaruh Perkembangan Teknologi Informasi Terhadap Peningkatan Kasus Kejahatan ITE Di Kabupaten Sinjai

Perkembangan teknologi informasi yang begitu pesat membawa kemudahan dalam berbagai aspek kehidupan manusia. Namun, kemajuan ini juga membuka peluang baru bagi terjadinya kejahatan, khususnya kejahatan siber atau cybercrime. Kejahatan ini memanfaatkan teknologi digital dan internet sebagai media melakukan tindakan ilegal yang merugikan individu maupun institusi. Dengan semakin luasnya penggunaan teknologi informasi, kasus kejahatan ITE di Indonesia juga mengalami peningkatan signifikan karena kemudahan akses dan kemampuan teknologi yang terus berkembang (Raodia, 2019).

Salah satu faktor penyebab peningkatan kasus kejahatan ITE adalah akses internet yang tidak terbatas dan risiko yang relatif kecil bagi pelaku. Kejahatan seperti penipuan online, hacking, pencurian data, penyebaran hoaks, dan tindakan merugikan lainnya dapat dilakukan dengan jarak jauh tanpa kontak langsung dengan korban. Sistem keamanan yang belum sepenuhnya kuat serta kurangnya kesadaran pengguna menjadi celah yang dimanfaatkan pelaku kejahatan untuk menjalankan aksinya. Hal ini membuat sangat penting adanya regulasi dan penerapan hukum yang ketat untuk mencegah dan menanggulangi kejahatan tersebut.

Pemerintah Indonesia merespon perkembangan kejahatan ini dengan mengeluarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) yang memberikan dasar hukum untuk penindakan kejahatan siber. UU ITE mengatur berbagai tindakan yang termasuk sebagai pelanggaran serta memperkuat mekanisme pembuktian dengan menetapkan alat bukti elektronik yang sah di pengadilan. Hal ini menjadikan proses penegakan hukum terhadap pelaku kejahatan ITE menjadi lebih efektif dan sesuai perkembangan teknologi yang ada (Rahmad, 2022).

Namun, penerapan hukum pun menghadapi tantangan, seperti minimnya sumber daya manusia (SDM) berkompeten di bidang teknologi informasi untuk penanganan kasus kejahatan ITE. Selain itu, karena karakteristik kejahatan siber yang melibatkan data digital dan sistem elektronik, penanganannya memerlukan keterampilan khusus dan pengetahuan teknologi yang mendalam. Oleh karena itu, peningkatan kapasitas aparat penegak hukum dan peningkatan kesadaran masyarakat sangat krusial dalam pengendalian kejahatan ini.

Peran teknologi itu sendiri bersifat ambivalen karena di satu sisi memudahkan aktivitas manusia, tapi di sisi lain menjadi alat untuk tindakan kriminal yang lebih kompleks. Perkembangan teknologi baru seperti kecerdasan buatan, big data, dan internet of things (IoT) jika disalahgunakan dapat menambah varian baru kejahatan ITE yang lebih susah dilacak dan ditangani. Contoh nyata seperti phishing yang memanipulasi informasi pribadi untuk tujuan kriminal makin marak terjadi seiring kemajuan teknologi tersebut (Supanto, 2016). Berikut beberapa kasus tentang Penyalahgunaan ITE di Kabupaten Sinjai:

a) Kasus Istri polisi jadi tersangka UU ITE di Sinjai (2023). Seorang istri polisi di Sinjai ditetapkan tersangka atas dugaan pelanggaran UU ITE, terkait pencemaran nama baik atau ujaran kebencian, setelah keluarganya ada kasus penembakan. Tersangka ditetapkan oleh penyidik Polda Sulawesi Selatan / unit siber.

b) Kasus Penipuan online modus "skema segitiga (sobis)" jual-beli cengkeh (2025). Pelaku berpura-pura membeli cengkeh lewat telepon/online, menggunakan identitas palsu dan rekening ilegal; korban pedagang cengkeh dirugikan sekitar Rp 200 jutaan. Enam pelaku ditetapkan tersangka; kasus dijerat dengan UU ITE (Pasal 28 ayat (1) jo Pasal 45 ayat (2) UU ITE), Pasal 55 KUHP.
c) Kasus Andi Darmawansyah dilaporkan oleh Bupati Sinjai atas postingan di media sosial (2021) Posting di medsos menuding pemotongan insentif & santunan COVID-19 dilaporkan sebagai pelanggaran ITE. Kasus ITE: ujaran/klaim melalui medsos dilaporkan ke polisi.

Perkembangan teknologi informasi telah membawa dampak signifikan terhadap peningkatan kasus kejahatan Informasi dan Transaksi Elektronik (ITE) di Kabupaten Sinjai. Kemajuan teknologi yang menjadikan komunikasi dan transaksi lebih mudah dan cepat juga membuka celah bagi pelaku kejahatan untuk melakukan tindak pidana di dunia maya, seperti pencemaran nama baik, penipuan online, dan kejahatan siber lainnya.

Hal ini disebabkan oleh akses yang semakin mudah ke berbagai aplikasi dan platform digital yang dapat disalahgunakan oleh oknum yang tidak bertanggung jawab, sehingga memicu lonjakan kasus kejahatan ITE di daerah tersebut. Selain itu, tantangan dalam pengawasan dan penanganan kejahatan ITE di Kabupaten Sinjai juga diperparah oleh respon birokrat yang masih lamban terhadap perkembangan teknologi informasi. Kondisi ini menyebabkan kesulitan dalam penegakan hukum dan pencegahan kriminalitas digital karena kurangnya pemahaman dan kesiapan aparat penegak hukum dalam menghadapi modus-modus kejahatan siber yang semakin canggih.

Oleh karena itu, dibutuhkan peningkatan sumber daya manusia yang terampil dan pemanfaatan teknologi yang maksimal untuk mengatasi permasalahan ini secara efektif. Berbagai jenis kejahatan ITE yang muncul antara lain pencemaran nama baik melalui media sosial, penipuan menggunakan teknologi digital, serta serangan melalui phishing dan malware. Studi-studi menunjukkan bahwa peningkatan kasus ini berkaitan langsung dengan perkembangan teknologi informasi yang tidak diimbangi dengan pengawasan dan edukasi yang memadai bagi masyarakat serta aparat penegak hukum. Untuk itu, penerapan UndangUndang ITE perlu disertai dengan upaya peningkatan kapasitas aparat serta kampanye literasi digital guna mencegah dan menangani kasus kejahatan siber di Kabupaten Sinjai secara menyeluruh.

Faktor-Faktor Yang Mempengaruhi Seseorang Untuk Melakukan Kejahatan ITE

Faktor-faktor yang memengaruhi seseorang melakukan kejahatan ITE antara lain adalah kelalaian pengguna, kelemahan sistem keamanan, anonimitas dan kemudahan akses internet, motif ekonomi atau pribadi, serta kurangnya kesadaran dan penegakan hukum. Faktor-faktor ini menciptakan celah dan kesempatan bagi pelaku untuk bertindak (Perbawa, 2021).

Perkembangan kejahatan berbasis teknologi informasi dan elektronik tidak dapat dilepaskan dari interaksi kompleks antara faktor teknis-sistemik dan faktor individual-sosial. Pada ranah teknis, kelemahan infrastruktur keamanan jaringan menjadi salah satu titik rawan yang paling dominan. Sistem yang tidak dirancang dengan standar proteksi mutakhir, minim pembaruan keamanan, serta lemahnya

mekanisme enkripsi dan autentikasi membuka celah eksploitasi yang luas bagi pelaku kejahatan siber. Kondisi ini menunjukkan bahwa transformasi digital yang tidak diiringi dengan penguatan arsitektur keamanan akan menghasilkan kerentanan struktural yang sistemik (Haryadi et al., 2024).

Kerentanan tersebut semakin diperparah oleh kelalaian pengguna sebagai aktor utama dalam ekosistem digital. Praktik penggunaan kata sandi yang sederhana, pengabaian verifikasi dua langkah, serta kebiasaan membagikan data pribadi tanpa pertimbangan risiko menjadi faktor yang memperbesar peluang terjadinya pelanggaran keamanan. Dalam konteks ini, persoalan keamanan siber tidak semata terletak pada teknologi, melainkan juga pada perilaku digital yang kurang bertanggung jawab (Putri, 2020).

Dinamika ini diperkuat oleh laju kemajuan teknologi yang sangat cepat. Inovasi di bidang kecerdasan buatan, komputasi awan, dan otomatisasi sistem memang memberikan kemudahan dan efisiensi, namun pada saat yang sama menghadirkan metode serangan baru yang lebih kompleks dan sulit terdeteksi. Ketidakseimbangan antara kecepatan inovasi teknologi dan kapasitas adaptasi sistem keamanan menciptakan kesenjangan proteksi yang dimanfaatkan oleh pelaku kejahatan (Benny, 2024). Akses internet yang semakin luas dan nyaris tanpa batas juga memperbesar ruang gerak pelaku. Ketersediaan jaringan yang terbuka memungkinkan aktivitas lintas wilayah tanpa hambatan geografis, sehingga memperumit upaya pengawasan dan penegakan hukum (Sumadi et al., n.d.).

Di sisi lain, faktor individu dan sosial memiliki kontribusi signifikan dalam menjelaskan fenomena kejahatan ITE. Anonimitas yang ditawarkan oleh ruang digital membentuk persepsi semu tentang keamanan diri. Pelaku merasa terlindungi oleh identitas virtual dan tidak mengalami konsekuensi sosial secara langsung, sehingga empati terhadap korban menjadi menurun (Anjani, 2024). Situasi ini melahirkan bentuk ketidakpedulian moral yang memperlemah kontrol sosial konvensional.

Motif ekonomi dan kepentingan pribadi juga menjadi pendorong utama. Keinginan memperoleh keuntungan finansial secara cepat, dorongan rasa ingin tahu terhadap celah sistem, hingga tindakan yang dilakukan sekadar untuk hiburan atau uji coba kemampuan teknis menunjukkan bahwa kejahatan ITE tidak bersifat tunggal, melainkan berlapis dan multidimensional (Rofiqoh, 2024). Selain itu, rendahnya kesadaran keamanan siber pada tingkat individu maupun organisasi memperparah risiko yang ada. Ketidaktahuan terhadap potensi ancaman, minimnya literasi digital, serta ketiadaan kebijakan keamanan internal membuat banyak pihak berada dalam posisi rentan terhadap eksploitasi (Budiyanto, 2025).

Faktor tersebut memperlihatkan bahwa kejahatan ITE merupakan hasil dari pertemuan antara kelemahan sistemik dan problematika perilaku manusia dalam ruang digital. Pendekatan penanggulangan yang efektif menuntut integrasi antara penguatan teknologi keamanan, peningkatan literasi digital, serta pembangunan kesadaran etis dalam penggunaan teknologi informasi.

A Dampak Kejahatan ITE Terhadap Masyarakat Di Kabupaten Sinjai

Kejahatan ITE memiliki dampak serius yang dirasakan langsung oleh masyarakat, terutama berupa kerugian ekonomi. Banyak individu maupun perusahaan menjadi korban kejahatan seperti pencurian data, penipuan online, dan peretasan sistem yang mengakibatkan kehilangan uang hingga miliaran rupiah. Dilaporkan bahwa kerugian ekonomi akibat kejahatan siber di Indonesia mencapai triliunan rupiah setiap tahunnya, yang mencerminkan betapa besar dampak finansial terhadap perekonomian masyarakat dan bisnis (Sidik, 2013).

Selain dampak ekonomi, kejahatan ITE juga menimbulkan dampak psikologis bagi korban. Korban penipuan online atau penyalahgunaan data pribadi sering mengalami stres, rasa takut, dan kehilangan kepercayaan terhadap penggunaan teknologi dan internet. Hal ini dapat mengurangi kenyamanan masyarakat dalam beraktivitas digital, bahkan memengaruhi kehidupan sosial dan keseharian mereka, terutama bagi mereka yang menjadi korban penyebaran konten negatif seperti hoaks dan fitnah di media sosial.

Dampak sosial lainnya adalah meningkatnya ketidakamanan di ruang digital yang berujung pada kebingungan dan keresahan masyarakat. Penyebaran informasi palsu dan ujaran kebencian dapat memecah belah masyarakat dan menimbulkan konflik sosial. Media sosial yang seharusnya menjadi sarana positif bagi komunikasi, terkadang menjadi ajang penyebaran kebencian yang dapat merusak keharmonisan sosial dan nilai-nilai kebersamaan di masyarakat. Keamanan data masyarakat menjadi salah satu isu utama yang terdampak oleh kejahatan ITE. Kebocoran data pribadi akibat peretasan atau malware membuat masyarakat rentan terhadap penyalahgunaan informasi seperti pencurian identitas dan penipuan. Kurangnya perlindungan data yang memadai menyebabkan masyarakat merasa tidak aman saat melakukan transaksi elektronik atau berbagi informasi melalui platform digital (Nuggraha, 2024).

Untuk menanggulangi dampak negatif tersebut, pemerintah telah mengeluarkan regulasi seperti Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) hingga Undang-Undang Perlindungan Data Pribadi. Regulasi ini berusaha memberikan perlindungan hukum bagi masyarakat serta meningkatkan kesadaran dan keamanan dalam penggunaan teknologi informasi. Namun, upaya edukasi dan penegakan hukum yang konsisten masih sangat diperlukan agar masyarakat dapat terlindungi secara maksimal dari kejahatan ITE. Dengan demikian, dampak kejahatan ITE terhadap masyarakat tidak hanya berdampak ekonomi, tetapi juga psikologis, sosial, dan keamanan data pribadi. Penting bagi semua pihak untuk meningkatkan kewaspadaan, edukasi, dan penguatan regulasi agar masyarakat dapat menikmati manfaat teknologi informasi dengan aman dan nyaman. Kejahatan ITE di Kabupaten Sinjai memberikan dampak negatif yang cukup signifikan terhadap masyarakat. Salah satunya adalah munculnya berbagai bentuk pencemaran nama baik melalui media sosial yang dapat merusak reputasi individu maupun kelompok secara luas. Hal ini menimbulkan ketidaknyamanan dan keresahan di tengah masyarakat karena informasi yang disebarkan seringkali sulit dikontrol dan berdampak lama secara sosial (Agung, 2025).

Selain aspek sosial, kejahatan ITE juga berdampak pada aspek keamanan dan ekonomi masyarakat. Praktik-praktik ilegal seperti penipuan online, pencurian data pribadi, dan peretasan akun membuat warga kehilangan kepercayaan terhadap penggunaan teknologi digital. Kejadian-kejadian tersebut dapat menyebabkan

kerugian materi yang tidak sedikit, serta menurunkan rasa aman dalam bertransaksi dan berkomunikasi secara elektronik. Lebih lanjut, dampak psikologis juga cukup besar dirasakan masyarakat Sinjai akibat kejahatan ITE. Korban kejahatan digital seperti ancaman, intimidasi, dan penyebaran konten negatif dapat mengalami stres, ketakutan, dan tekanan psikologis yang berlarut-larut. Oleh karena itu, upaya sosialisasi dan penegakan hukum yang efektif sangat diperlukan untuk melindungi masyarakat dan mendorong penggunaan teknologi informasi secara sehat dan aman di Kabupaten Sinjai.

Strategi Pencegahan Kejahatan ITE Yang Efektif Di Era Digital

Strategi pencegahan kejahatan Informasi dan Transaksi Elektronik (ITE) yang efektif di era digital melibatkan pendekatan holistik, yang mencakup peningkatan literasi digital, penguatan keamanan teknis, dan pemahaman aspek hukum. Berikut adalah empat strategi utama untuk pencegahan kejahatan ITE yang efektif:

1. Peningkatan Literasi dan Kesadaran Digital

   Peningkatan literasi dan kesadaran digital dilakukan melalui berbagai pendekatan, seperti integrasi dalam kurikulum pendidikan, pelatihan bagi guru dan orang tua, kampanye publik, serta pemanfaatan teknologi untuk literasi. Tujuannya adalah membekali masyarakat dengan kemampuan berpikir kritis, mengakses informasi akurat, menjaga privasi, berkomunikasi secara efektif, dan memanfaatkan teknologi secara bijak dan aman.

   a) Edukasi Masyarakat: Melakukan kampanye kesadaran tentang berbagai modus kejahatan siber, seperti penipuan phishing, pembobolan rekening, dan penyebaran hoaks.
   b) Berpikir Kritis: Mendorong pengguna internet untuk selalu memverifikasi informasi dan tidak mudah percaya atau langsung mengeklik tautan yang mencurigakan.
   c) Memahami Etika Digital: Menanamkan kesadaran etis dalam penggunaan teknologi secara bijak dan bertanggung jawab, menghindari penyalahgunaan kemampuan teknis untuk tujuan negatif.

2. Penguatan Keamanan Teknis Individual

   Penguatan Keamanan Teknis Individual mengacu pada serangkaian tindakan dan praktik yang dilakukan individu untuk melindungi informasi pribadi, perangkat, dan aktivitas online mereka dari ancaman digital. Ini adalah pendekatan proaktif untuk meminimalkan risiko menjadi korban kejahatan siber seperti peretasan, pencurian identitas, penipuan *phishing, dan malware.* Pengguna harus menerapkan langkahlangkah teknis dasar untuk melindungi data dan perangkat pribadi mereka.

   a) Kata Sandi Kuat dan Unik, Gunakan kata sandi yang kompleks dan berbeda untuk setiap akun. Pertimbangkan penggunaan pengelola kata sandi (*password manager).*
   b) Autentikasi Dua Faktor (2FA), Aktifkan 2FA di semua akun yang mendukungnya untuk lapisan keamanan tambahan.
   c) Pembaruan Perangkat Lunak Berkala, Pastikan sistem operasi dan aplikasi selalu diperbarui untuk menambal celah keamanan yang mungkin dieksploitasi oleh peretas. o Waspada *Wi-Fi* Publik: Hindari

mengakses informasi sensitif (seperti perbankan) saat menggunakan jaringan *Wi-Fi* publik yang tidak aman.

3. Kolaborasi Antar Pihak (Pemerintah, Swasta, dan Masyarakat) Kolaborasi antara pemerintah, sektor swasta, dan masyarakat sangat penting dan merupakan kunci dalam menghadapi kejahatan siber. Di Indonesia, pendekatan *multistakeholder* ini didorong untuk mewujudkan ketahanan siber nasional
    a) Sinkronisasi Regulasi: Pemerintah perlu memastikan sinkronisasi antara UU ITE dan regulasi terkait lainnya, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), untuk landasan hukum yang kuat.
    b) Peningkatan Kapasitas Penegak Hukum: Pihak berwenang, khususnya kepolisian siber, dituntut untuk terus beradaptasi dan meningkatkan kemampuan forensik digital mereka dalam menangani kasus kejahatan ITE.
    c) Respons Cepat dan Pelaporan: Membangun mekanisme pelaporan yang efisien agar korban kejahatan digital dapat segera menghubungi pihak berwenang atau layanan pelanggan terkait untuk bantuan.

4. Penerapan Teknologi Keamanan

    Penerapan teknologi keamanan dalam kejahatan siber mencakup penggunaan sistem deteksi dan respons otomatis, enkripsi data, otentikasi dua faktor, dan pembaruan perangkat lunak rutin. Teknologi kecerdasan buatan (AI) sangat membantu dalam menganalisis pola perilaku jaringan dan mendeteksi ancaman secara real-time, sementara kriptografi melindungi kerahasiaan data. Selain itu, keamanan siber juga bergantung pada kebiasaan pengguna, seperti menggunakan kata sandi kuat dan berhati-hati terhadap phishing.
    a) Penggunaan *Firewall* dan Antivirus: Menggunakan perangkat lunak keamanan seperti firewall dan program antivirus yang mutakhir untuk melindungi jaringan dan perangkat dari serangan.
    b) Enkripsi Data: Menerapkan enkripsi untuk menjaga kerahasiaan data sensitif, baik saat disimpan maupun saat dikirimkan melalui internet.
    c) Pencadangan Data Berkala: Melakukan pencadangan data secara berkala untuk meminimalkan kerugian jika terjadi serangan siber seperti *ransomware.*

KESIMPULAN

Salah satu faktor penyebab peningkatan kasus kejahatan ITE adalah akses internet yang tidak terbatas dan risiko yang relatif kecil bagi pelaku. Kejahatan seperti penipuan online, *hacking*, pencurian data, penyebaran *hoaks,* dan tindakan merugikan lainnya dapat dilakukan dengan jarak jauh tanpa kontak langsung dengan korban. Sistem keamanan yang belum sepenuhnya kuat serta kurangnya kesadaran pengguna menjadi celah yang dimanfaatkan pelaku kejahatan untuk menjalankan aksinya. Hal ini membuat sangat penting adanya regulasi dan penerapan hukum yang ketat untuk mencegah dan menanggulangi kejahatan tersebut . Faktor-faktor ini menciptakan celah dan kesempatan bagi pelaku untuk bertindak Kejahatan ITE memiliki dampak serius yang dirasakan langsung oleh masyarakat di Kabupaten Sinjai, terutama berupa

kerugian ekonomi. Banyak individu maupun perusahaan menjadi korban kejahatan seperti pencurian data, penipuan online, dan peretasan sistem yang mengakibatkan kehilangan uang hingga miliaran rupiah. Di Era Digital Penerapan teknologi keamanan dalam kejahatan siber mencakup penggunaan sistem deteksi dan respons otomatis, enkripsi data, otentikasi dua faktor, dan pembaruan perangkat lunak rutin. Teknologi kecerdasan buatan (AI) sangat membantu dalam menganalisis pola perilaku jaringan dan mendeteksi ancaman secara real-time, sementara kriptografi melindungi kerahasiaan data. Selain itu, keamanan siber juga bergantung pada kebiasaan pengguna, seperti menggunakan kata sandi kuat dan berhati-hati terhadap *phishing*.

DAFTAR PUSTAKA

Aabid, M., Dzaky, T., & Edrisy, I. F. (2025). *Strategi Pencegahan Kejahatan Siber di Indonesia : Sinergi antara UU ITE dan Kebijakan Keamanan Digital*. *4*(2), 3614–3625.

Agung, A. (2025). *Kejahatan Informasi dan transaksi elektronik*. 3, 1–29.

Anjani, V. A. (2024). *Cyberbullying dan Dinamika Hukum di Indonesia : Paradoks Ruang Maya dalam Interaksi Sosial di Era Digital Pendahuluan membawa transformasi besar dalam cara manusia berkomunikasi dan*. 4(1), 1–28.

Abdoellah, 2024, *Terdesak kebutuhan keluarga, 2 mama muda di Sinjai nekat jajakan diri, OkeZoneNews*, 21 April 2024, https://news.okezone.com/amp/2024/04/21/340/2998690/terdesak-kebutuhan-keluarga-2-mamah-muda-di-sinjai-nekat-jajakan-diri

Benny, V. (2024). Sistem Keamanan Informasi.

Budiyanto, D., Mabruri, M., Studi, P., Informasi, S., & Jember, U. T. (2025). Pentingnya keamanan siber dalam era digital: tinjauan global dan kondisi di indonesia. 2(1), 981–994.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. 2(2). https://doi.org/10.21143/TELJ.vol2.no2.1043

Franklin. (2013). PERTANGGUNGJAWABAN BANK TERHADAP NASABAH YANG MENJADI KORBAN KEJAHATAN INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE). 1.

Farid Asifa, 2023, Kronologi Istri Polisi Jadi Tersangka UU ITE, Berawal Kekecewaan Sang Kakak Ditembak Mati Polres Sinjai, Kompas.com, 7 Maret 2023,
https://makassar.kompas.com/read/2023/03/07/102446478/kronologi-istri-polisi-jadi-tersangka-uu-ite-berawal-kekecewaan-sang-kakak?page=all

Haryadi, E., Wijayanti, D., Ramdhani, E. C., Widyastuti, I., Informasi, P. S., & Akuntansi, P. S. (2024). IDENTIFIKASI ANCAMAN KEAMANAN SIBER DARI PENYALAHGUNAAN SUMBER DAYA TIK : STUDI KASUS. 14(4), 886–896.

Indonesia, R. (2008). UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008.

Informasi, E. U., & Transaksi, D. A. N. (2008). Efektivitas undang-undang informasi dan transaksi elektronik di indonesia dalam aspek hukum pidana. 2(2), 139–146.

Munajat, A. A., & Yusuf, H. (2024). Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus : Studi Tentang Kejahatan Keuangan Berbasis Digital The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes : A Study of Digital-Based Financial Crimes. November, 4853– 4865.

Nuggraha, A., Muliya, A. B., Aulia, F., Teguh, S. A., Masyarakat, I., & Sosial, M. (2024). Dampak UU ITE Terhadap Interaksi Masyarakat Di Media Sosial. 21–33. https://doi.org/10.70656/lsj.v1i2.130

Perbawa, P. (2021). CRIME YANG DILAKUKAN OLEH ORANG ASING DI BALI DITINJAU DARI PERSPEKTIF KRIMINOLOGI. 01(01), 58–70.

Putri, A. (2020). Perlindungan Hukum Pengguna Marketplace Dalam Hal Keamanan Data Pribadi Pengguna.

Rahmad, N., Arifah, K. N., Setiyawan, D., Ramli, M., & Daud, B. S. (2022). Efektivitas Bukti Elektronik Dalam Uu Ite Sebagai Perluasan Sistem Pembuktian Dalam Kuhap Efektivitas Bukti Elektronik Dalam Uu Ite Sebagai Perluasan Sistem Pembuktian Dalam Kuhap. 96–111.

Rahmanto, T. Y. (2019). PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PENIPUAN BERBASIS TRANSAKSI ELEKTRONIK. 19(30), 31–52.

Raodia. (2019). Pengaruh perkembangan teknologi terhadap terjadinya kejahatan mayantara (cybercrime). 6, 230–239.

Razzaq, A., Aditya, M., Widya, A., Kuncoro, O., Lesmana, D., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus : Predator). 6(April), 35–46. https://doi.org/10.34010/gpsjournal.v6i1

Rofiqoh. (2024). Mengupas Fenomena Cybercrime dalam Ranah Hukum Pidana Ekonomi: Menghadirkan Tantangan Baru bagi Penegakan Hukum di Era Digital.

Setiawan, D. A. (2024). STRATEGI PENANGGULANGAN KEJAHATAN EKONOMI BERBASIS TEKNOLOGI : STUDI KOMPARATIF ANTARA INDONESIA , AMERIKA , DAN EROPA.53, 78–89.

Sidik, S. (2013). Dampak undang-undang informasi dan transaksi elektronik (uu ite) terhadap perubahan hukum dan sosial dalam masyarakat. 1.

Suhartini, E. (2016). ANALISIS KEPASTIAN HUKUM ALAT BUKTI PADA PERJANJIAN ELEKTRONIK BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. 2(1), 23–41.

Sumadi, H., Hukum, F., & Subang, U. (n.d.). Kendala dalam menanggulangi tindak pidana penipuan transaksi elektronik di indonesia. 33(2).

Supanto. (2016). PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY. 5(1).

Tulla, 2025, Penipuan skema segitiga di sinjai dibongkar polisi, BeritaSulSel.com, 18 Februari 2025, https://beritasulsel.com/baca/penipuan-skema-segitiga-di-sinjai-dibongkar-polisi-korban-tertipu-rp200-juta

Udayana, U., Klod, D. P., & Denpasar, K. (2025). ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA. 3(2).

UU Tahun 2008 tentang Informasi dan Transaksi Elektronik.

UU Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Walintukan, S. J. (2022). AKIBAT HUKUM BAGI PELAKU PENYADAPAN ILEGAL (INTERSEPSI) MENURUT UNDANG- UNDANG TELEKOMUNIKASI SERTA UNDANG- UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK. XI(1), 5–14.

Winarni, R. R. (2016). Efektifitas Penerapan UU ITE Dalam Tindakan Pidana Cyber Crime. 14(0854), 16–27.

Zulkipli, 2021, Warga yang Dilaporkan Bupati Sinjai Gegara Postingan Jadi Tersangka UU ITE, BeritaNews, 20 agustus 2021, https://news.detik.com/berita/d-5690325/warga-yang- dilaporkan-bupati-sinjai-gegara-postingan-jadi-tersangka-uu-ite