Lawful Interception dalam Penegakan Keamanan Siber di Indonesia: Analisis Hukum Normatif dan Implikasi Teknis terhadap Integritas Bukti Digital dan Pengawasan

Ade Mulya[1) *], Prasetyo Adi Wibowo Putro[2] , Muhammad Ghani Nurramdhan[3)]

1) Kepolisian Negara Republik Indonesia. Jakarta, ade.mulya@polri.go.id
2) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, prasetyo.adi@poltekssn.ac.id
3) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, muhammad.ghani@student.poltekssn.ac.id

Riwayat Artikel

Dikirim 18 Jan 2026
Diterima 21 Apr 2026
Diterbitkan 28 Apr 2026

Kata kunci:

lawful interception
keamanan siber
bukti digital
forensik digital
regulasi

Keywords:

lawful interception
cybersecurity
digital evidence
digital forensic
regulation

Abstrak

Perkembangan pesat teknologi komunikasi digital, termasuk enkripsi ujung-ke-ujung dan infrastruktur jaringan berkecepatan tinggi, telah meningkatkan kompleksitas kejahatan siber dan tantangan dalam mengumpulkan bukti digital yang andal. Intersepsi Hukum (*Lawful Interception*/LI) merupakan instrumen penting bagi penegakan hukum; namun, implementasinya menimbulkan masalah regulasi dan teknis yang memengaruhi keamanan komunikasi dan integritas bukti. Studi ini bertujuan untuk menganalisis kerangka regulasi LI di Indonesia dan mengevaluasi implikasinya terhadap keamanan siber dan keandalan forensik digital. Penelitian ini menggunakan pendekatan hukum normatif yang dikombinasikan dengan analisis implikasi teknis untuk menilai konsistensi regulasi dengan prinsip-prinsip keamanan siber dan standar forensik digital. Hasil penelitian menunjukkan bahwa regulasi LI di Indonesia masih terfragmentasi, dengan ketentuan yang tidak konsisten mengenai otorisasi, pengawasan, dan manajemen data. Kesenjangan ini menciptakan kerentanan dalam kontrol teknis, melemahkan pemisahan tugas, dan meningkatkan risiko terhadap integritas dan rantai penguasaan bukti digital. Studi ini menyimpulkan bahwa harmonisasi regulasi yang selaras dengan prinsip-prinsip keamanan siber sangat penting untuk memastikan bukti digital yang andal dan penegakan hukum siber yang efektif. Kontribusi penelitian ini adalah pengembangan pendekatan evaluasi integratif yang menghubungkan analisis regulasi dengan perspektif keamanan siber dan forensik digital dalam menilai praktik penyadapan yang sah.

Abstract

The rapid development of digital communication technologies, including end-to-end encryption and high-speed network infrastructures, has increased the complexity of cybercrime and challenges in collecting reliable digital evidence. Lawful Interception (LI) is a critical instrument for law enforcement; however, its implementation raises regulatory and technical issues affecting communication security and evidence integrity. This study aims to analyze the regulatory framework of LI in Indonesia and evaluate its implications for cybersecurity and digital forensic reliability. The research employs a normative legal approach combined with technical implications analysis to assess regulatory consistency with cybersecurity principles and digital forensic standards. The results show that LI regulations in Indonesia remain

fragmented, with inconsistent provisions on authorization, oversight, and data management. These gaps create vulnerabilities in technical control, weaken separation of duties, and increase risks to the integrity and chain of custody of digital evidence. This study concludes that regulatory harmonization aligned with cybersecurity principles is essential to ensure reliable digital evidence and effective cyber law enforcement. The contribution of this study is the development of an integrative evaluation approach that links regulatory analysis with cybersecurity and digital forensic perspectives in assessing lawful interception practices.

1. PENDAHULUAN

Perkembangan teknologi komunikasi digital yang pesat, ditandai dengan pemanfaatan layanan berbasis internet, enkripsi *end-to-end*, serta jaringan berkecepatan tinggi, telah meningkatkan kompleksitas kejahatan siber dan tantangan dalam penegakan hukum. Kejahatan serius dan tindak pidana siber semakin mengandalkan media komunikasi digital yang aman dan sulit diakses melalui metode investigasi konvensional, sehingga menuntut penggunaan mekanisme intersepsi komunikasi sebagai bagian dari upaya pengamanan ruang siber dan pengumpulan bukti digital [1][2]. Dalam konteks ini, *Lawful Interception* (LI) dipahami sebagai instrumen penegakan hukum yang sah untuk memperoleh data komunikasi yang relevan dalam penyelidikan tindak pidana berbasis teknologi informasi.

Sejumlah penelitian menunjukkan bahwa penerapan LI tidak hanya berkaitan dengan aspek teknis intersepsi jaringan, tetapi juga memiliki implikasi langsung terhadap keamanan sistem komunikasi dan keandalan bukti digital. Studi sebelumnya menyoroti tantangan teknis LI dalam lingkungan komunikasi terenkripsi, termasuk keterbatasan akses terhadap konten komunikasi serta potensi degradasi integritas data [3]. Pada sisi lain, literatur forensik digital menegaskan bahwa keabsahan bukti digital sangat bergantung pada kepastian prosedur, pengawasan teknis, serta kejelasan rantai penguasaan (*chain of custody*) sejak tahap akuisisi hingga pembuktian di pengadilan [4].

Meskipun demikian, sebagian besar kajian terkait LI masih berkembang secara terpisah antara perspektif hukum dan aspek teknis. Studi hukum cenderung berfokus pada isu legalitas dan perlindungan hak asasi, sementara kajian teknis lebih menekankan pada keterbatasan intersepsi dalam lingkungan komunikasi terenkripsi. Kondisi ini menunjukkan adanya kesenjangan analitis dalam memahami bagaimana desain regulasi LI secara langsung mempengaruhi keamanan sistem komunikasi digital serta keandalan bukti digital dalam praktik forensik siber. Kesenjangan ini menjadi signifikan karena validitas bukti digital tidak hanya ditentukan oleh dasar hukum, tetapi juga oleh bagaimana regulasi tersebut membentuk proses teknis intersepsi, pengelolaan data, serta rantai penguasaan bukti secara menyeluruh [3][4].

Dalam konteks nasional, pengaturan LI di Indonesia masih bersifat terfragmentasi dan tersebar dalam berbagai peraturan sektoral serta regulasi internal aparat penegak hukum. Kondisi ini telah dikritisi karena berpotensi menimbulkan ketidakpastian hukum, perbedaan standar teknis intersepsi, serta lemahnya mekanisme pengawasan independen [5]. Mahkamah Konstitusi melalui Putusan Nomor 5/PUU-VIII/2010 menegaskan bahwa penyadapan sebagai pembatasan hak berkomunikasi harus diatur secara jelas dalam undang-undang guna mencegah penyalahgunaan kewenangan dan menjaga akuntabilitas penegakan hukum [6]. Namun, ketidakharmonisan antara mandat konstitusional tersebut dan praktik regulasi yang ada berpotensi berdampak pada keamanan sistem komunikasi digital serta keabsahan bukti digital hasil intersepsi.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis kerangka regulasi LI di Indonesia serta mengevaluasi implikasinya terhadap keamanan komunikasi digital, integritas bukti digital, dan keandalan proses forensik siber dalam penegakan hukum. Penelitian ini juga berupaya mengisi kesenjangan kajian dengan mengintegrasikan perspektif hukum dan keamanan siber dalam satu kerangka analisis yang komprehensif.

Secara ilmiah, penelitian ini memberikan kontribusi dengan mengembangkan pendekatan evaluasi regulasi LI berbasis prinsip keamanan siber dan forensik digital. Berbeda dengan kajian sebelumnya yang cenderung menempatkan LI dalam kerangka hukum atau hak asasi manusia semata, penelitian ini memosisikan regulasi sebagai bagian dari desain sistem keamanan siber yang memiliki implikasi langsung terhadap *attack surface, trust boundary*, serta integritas bukti digital. Dengan demikian, penelitian ini tidak hanya memperluas perspektif kajian LI, tetapi juga menawarkan pendekatan integratif yang menghubungkan analisis normatif hukum dengan evaluasi teknis-konseptual keamanan siber dalam konteks penegakan hukum digital.

Kontribusi penelitian ini adalah:

[1] mengidentifikasi kelemahan struktural dalam regulasi *Lawful Interception* di Indonesia dari perspektif keamanan siber;

[2] mengevaluasi implikasi regulasi terhadap integritas bukti digital dan *chain of custody* dalam praktik forensik siber; dan

[3] menawarkan pendekatan analitis integratif yang menghubungkan regulasi hukum dengan prinsip keamanan siber dan kesiapan forensik digital.

2. LANDASAN TEORI

2.1. Lawful Interception sebagai Instrumen Keamanan Siber

LI dipahami sebagai mekanisme intersepsi komunikasi yang dilakukan secara sah oleh aparat penegak hukum untuk kepentingan penyelidikan dan penegakan hukum. Dalam konteks keamanan siber, LI berfungsi sebagai instrumen untuk memperoleh informasi strategis terkait aktivitas kejahatan siber yang memanfaatkan jaringan komunikasi digital sebagai medium utama [7]. Berbeda dengan kegiatan intelijen strategis, LI ditempatkan sebagai bagian dari proses penegakan hukum (*pro justitia*) yang harus tunduk pada batasan hukum dan prosedural yang jelas. Oleh karena itu, penerapan LI tidak hanya dipengaruhi oleh kemampuan teknis intersepsi, tetapi juga oleh kerangka regulasi yang menentukan legitimasi dan ruang lingkup penggunaannya.

Dalam literatur keamanan siber, LI juga dipandang sebagai komponen dari tata kelola keamanan siber, yaitu tata kelola keamanan siber yang melibatkan interaksi antara teknologi, kebijakan, dan institusi [8]. Ketidaksesuaian antara regulasi dan perkembangan teknologi komunikasi, seperti penggunaan enkripsi *end-to-end*, dapat melemahkan efektivitas LI sekaligus meningkatkan risiko penyalahgunaan kewenangan. Dengan demikian, teori mengenai LI dalam keamanan siber menekankan perlunya keseimbangan antara kebutuhan pengamanan ruang siber dan perlindungan hak dasar pengguna sistem komunikasi digital.

2.2. Regulasi Lawful Interception dan Prinsip Legalitas

Regulasi LI merupakan fondasi utama dalam menentukan batasan, prosedur, dan otoritas yang berwenang melakukan intersepsi komunikasi. Prinsip legalitas menuntut agar setiap tindakan penyadapan memiliki dasar hukum yang jelas, dapat diprediksi, dan dapat diuji secara hukum [9]. Dalam konteks negara hukum, regulasi LI tidak hanya berfungsi sebagai alat legitimasi, tetapi juga sebagai mekanisme pembatas kekuasaan agar intersepsi komunikasi tidak dilakukan secara sewenang-wenang.

Sejumlah kajian menunjukkan bahwa fragmentasi regulasi LI berpotensi menimbulkan ketidakpastian hukum dan perbedaan standar penerapan antar lembaga penegak hukum [10]. Kondisi tersebut dapat berdampak pada lemahnya akuntabilitas dan pengawasan terhadap praktik intersepsi komunikasi, terutama dalam lingkungan komunikasi digital yang kompleks. Oleh karena itu, teori regulasi LI menekankan pentingnya harmonisasi aturan dan kejelasan mekanisme pengawasan sebagai prasyarat bagi penegakan hukum yang sah dan efektif di ranah siber.

2.3. Keamanan Komunikasi Digital dan Tantangan Enkripsi

Keamanan komunikasi digital merupakan elemen kunci dalam ekosistem keamanan siber modern. Penggunaan teknologi enkripsi, khususnya enkripsi *end-to-end*, dirancang untuk melindungi kerahasiaan dan integritas komunikasi dari akses tidak sah [19]. Namun, dari perspektif penegakan hukum, enkripsi juga menghadirkan tantangan signifikan dalam pelaksanaan LI karena membatasi kemampuan aparat untuk mengakses konten komunikasi meskipun telah memiliki otorisasi hukum.

Literatur keamanan siber menyoroti bahwa ketegangan antara perlindungan enkripsi dan kebutuhan intersepsi komunikasi merupakan isu struktural yang belum sepenuhnya terselesaikan [11]. Upaya untuk melemahkan enkripsi demi kepentingan intersepsi berpotensi menurunkan tingkat keamanan sistem komunikasi secara keseluruhan. Oleh karena itu, teori keamanan komunikasi digital menempatkan LI sebagai variabel yang harus dikelola secara hati-hati agar tidak menciptakan kerentanan baru dalam infrastruktur komunikasi digital.

2.4. Bukti Digital dan Prinsip Forensik Digital

Bukti digital merupakan informasi yang dihasilkan, disimpan, atau ditransmisikan melalui sistem elektronik dan digunakan dalam proses pembuktian hukum. Dalam konteks kejahatan siber, bukti digital sering kali menjadi elemen kunci yang menentukan keberhasilan penegakan hukum [12]. Forensik digital berfungsi sebagai disiplin ilmu yang memastikan bahwa proses pengumpulan, penyimpanan, dan analisis bukti digital dilakukan secara sistematis, akurat, dan dapat dipertanggungjawabkan.

Prinsip utama dalam forensik digital mencakup integritas data, keaslian bukti, dan kejelasan rantai penguasaan [13]. Bukti digital yang diperoleh melalui LI harus memenuhi prinsip-prinsip tersebut agar dapat diterima dan dipercaya dalam proses peradilan. Dengan demikian, teori forensik digital memberikan kerangka evaluasi untuk menilai apakah praktik LI telah selaras dengan standar pengelolaan bukti digital yang andal.

2.5. Pengawasan dan Akuntabilitas dalam Praktik Lawful Interception

Pengawasan dan akuntabilitas merupakan elemen penting dalam teori tata kelola keamanan siber, khususnya dalam penerapan instrumen koersif seperti LI. Tanpa mekanisme pengawasan yang memadai, LI berpotensi disalahgunakan dan menimbulkan dampak negatif terhadap kepercayaan publik serta legitimasi penegakan hukum [14]. Dalam literatur, pengawasan dapat dilakukan melalui mekanisme internal, yudisial, maupun lembaga independen yang memiliki kewenangan evaluatif.

Akuntabilitas praktik LI juga berkaitan erat dengan transparansi prosedur dan dokumentasi teknis intersepsi komunikasi [15]. Dalam konteks forensik digital, akuntabilitas menjadi prasyarat untuk memastikan bahwa bukti digital hasil intersepsi dapat diaudit dan diverifikasi secara independen. Oleh karena itu, teori pengawasan LI menekankan pentingnya integrasi antara regulasi, mekanisme kontrol, dan standar teknis untuk menjamin keamanan siber dan keandalan bukti digital.

3. METODE PENELITIAN

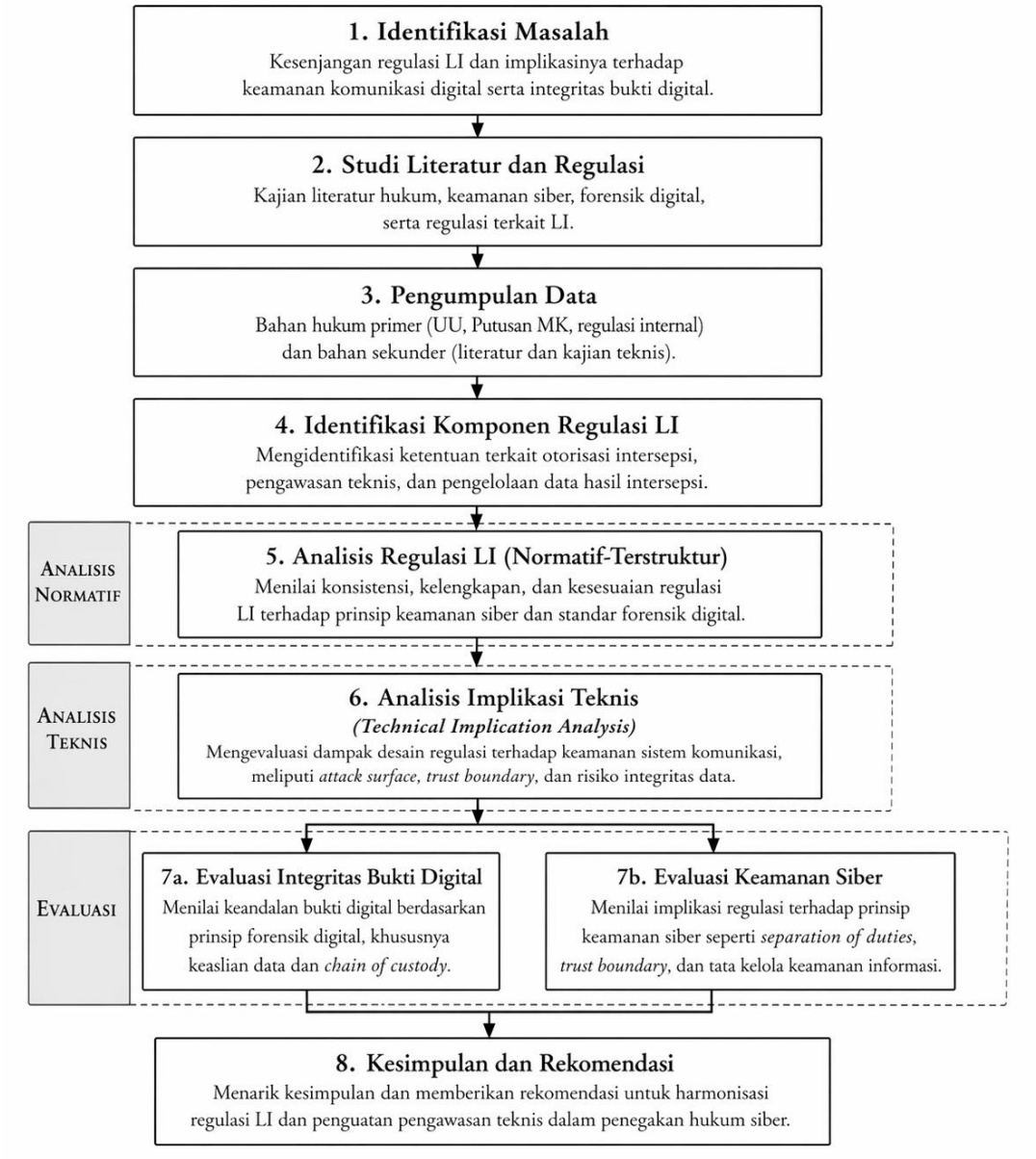
Penelitian ini menggunakan pendekatan hukum normatif yang diperkaya dengan analisis teknis konseptual keamanan siber untuk mengevaluasi keterkaitan antara kerangka regulasi *Lawful Interception* (LI) dan implikasinya terhadap keamanan komunikasi digital serta keandalan bukti digital. Pendekatan ini dipilih karena penelitian tidak berfokus pada pengujian performa sistem, melainkan pada analisis keterulangan prosedural (*procedural reproducibility*) dalam praktik intersepsi komunikasi dan pengelolaan bukti digital [16].

Metode yang digunakan adalah analisis normatif-terstruktur terhadap regulasi LI di Indonesia, yang mencakup peraturan perundang-undangan dan regulasi internal aparat penegak hukum. Analisis dilakukan dengan menilai konsistensi regulasi terhadap prinsip keamanan siber dan standar forensik digital, khususnya pada aspek otorisasi, pengawasan, serta pengelolaan data hasil intersepsi [4][5][6]. Untuk melengkapi analisis tersebut, digunakan *technical implication analysis* guna

mengevaluasi implikasi desain regulasi terhadap keamanan sistem komunikasi, termasuk potensi *attack surface, trust boundary*, serta risiko terhadap integritas data [17].

Pengumpulan data dilakukan melalui studi kepustakaan dengan menggunakan bahan hukum primer dan sekunder yang relevan dengan intersepsi komunikasi dan pengelolaan bukti digital. Analisis data dilakukan secara kualitatif-terstruktur melalui tahapan: (1) identifikasi komponen regulasi, (2) analisis regulasi, (3) analisis implikasi teknis, serta (4) evaluasi terhadap integritas bukti digital dan keamanan siber berdasarkan prinsip forensik digital [12][13].

Alur metodologi penelitian disajikan pada Gambar 1, yang menggambarkan keterkaitan antara analisis regulasi, analisis implikasi teknis, serta evaluasi terhadap integritas bukti digital dan keamanan siber dalam penegakan hukum siber.



Gambar 1. Alur metodologi penelitian

4. HASIL DAN PEMBAHASAN

4.1. Hasil Analisis Regulasi Lawful Interception di Indonesia

Hasil analisis terhadap regulasi LI di Indonesia menunjukkan bahwa pengaturan intersepsi komunikasi masih bersifat terfragmentasi dan tersebar dalam berbagai peraturan sektoral serta

regulasi internal aparat penegak hukum. Tidak ditemukan satu kerangka regulasi terpadu yang secara konsisten mengatur aspek otorisasi, pelaksanaan teknis, pengawasan, dan pengelolaan hasil intersepsi sebagai bukti digital. Kondisi ini menyebabkan variasi prosedural dalam praktik LI, terutama terkait mekanisme pemberian izin dan dokumentasi teknis intersepsi [5][6].

Analisis lebih lanjut menunjukkan bahwa dalam regulasi internal, khususnya pada tingkat operasional, kewenangan otorisasi penyadapan cenderung ditempatkan dalam struktur internal institusi penegak hukum. Model ini menghasilkan konsentrasi kewenangan pada satu entitas yang berperan sebagai pemohon, pelaksana, dan pengendali teknis intersepsi. Dari perspektif keamanan siber, temuan ini mengindikasikan lemahnya pemisahan peran (*separation of duties*) yang merupakan prinsip penting dalam pengamanan sistem dan pengelolaan data sensitif [18].

4.2. Hasil Analisis Implikasi Teknis Lawful Interception terhadap Keamanan Komunikasi

Hasil analisis teknis menunjukkan bahwa perkembangan teknologi komunikasi digital, khususnya penggunaan enkripsi *end-to-end* dan layanan komunikasi berbasis internet, membatasi kemampuan akses langsung terhadap konten komunikasi dalam praktik LI. Intersepsi pada lapisan jaringan sering kali hanya menghasilkan metadata komunikasi, sementara konten tetap terlindungi oleh mekanisme kriptografi yang kuat [19]. Kondisi ini berdampak pada efektivitas LI dalam memperoleh bukti digital yang relevan secara substansial.

Selain keterbatasan akses konten, hasil analisis juga menunjukkan adanya potensi risiko keamanan pada titik intersepsi (*interception point*). Setiap mekanisme LI memerlukan titik akses khusus yang, apabila tidak dikelola dengan standar keamanan yang memadai, dapat memperluas *attack surface* sistem komunikasi. Risiko ini mencakup kemungkinan akses tidak sah, kebocoran data hasil intersepsi, serta manipulasi data yang berdampak langsung pada integritas bukti digital [20].

Untuk merangkum hasil analisis terhadap karakteristik pengaturan LI di Indonesia dan implikasinya terhadap keamanan siber serta keandalan bukti digital, dilakukan pemetaan aspek-aspek kunci regulasi yang relevan. Pemetaan tersebut disajikan pada Tabel 1, yang menunjukkan keterkaitan antara desain regulasi LI, mekanisme otorisasi dan pengawasan, serta potensi dampaknya terhadap integritas bukti digital dan praktik forensik siber.

Tabel 1. Pemetaan Regulasi LI di Indonesia dan Karakteristik Otorisasi

Aspek Pengaturan	**Karakteristik Regulasi** LI	**Implikasi terhadap Keamanan Siber dan Bukti Digital**
Dasar hukum intersepsi	Tersebar dalam berbagai peraturan sektoral dan regulasi internal aparat penegak hukum	Menimbulkan ketidakseragaman standar teknis dan prosedural intersepsi
Otorisasi penyadapan	Umumnya diberikan melalui mekanisme internal lembaga penegak hukum	Berpotensi melemahkan prinsip pemisahan peran (*separation of duties*)
Pengawasan pelaksanaan	Tidak diatur secara seragam; pengawasan eksternal terbatas	Meningkatkan risiko penyalahgunaan kewenangan dan lemahnya akuntabilitas teknis
Pengelolaan hasil intersepsi	Ketentuan teknis penyimpanan dan pengamanan data tidak dirumuskan secara rinci	Berpotensi mengganggu integritas bukti digital dan keamanan data hasil intersepsi
Rantai penguasaan	Belum diatur secara eksplisit dalam seluruh regulasi LI	Menimbulkan risiko sengketa keabsahan bukti digital dalam proses forensik
Audit dan verifikasi teknis	Tidak terdapat kewajiban audit teknis independen	Menyulitkan verifikasi integritas dan keandalan bukti digital

4.3. Diskusi: Dampak Regulasi Lawful Interception terhadap Integritas Bukti Digital

Temuan penelitian ini menunjukkan bahwa fragmentasi regulasi dan keterbatasan pengawasan teknis dalam praktik LI memiliki implikasi langsung terhadap integritas bukti digital. Bukti digital hasil LI sangat bergantung pada kejelasan prosedur akuisisi, penyimpanan, dan dokumentasi teknis sejak tahap awal intersepsi. Ketidakkonsistenan regulasi berpotensi menghasilkan variasi standar operasional yang berdampak pada keandalan bukti dalam proses forensik digital [21].

Temuan ini sejalan dengan literatur forensik digital yang menekankan bahwa kesalahan prosedural, ketidakpastian proses, dan kehilangan kontrol terhadap data dapat menyebabkan degradasi nilai pembuktian bukti digital [21]. Selain itu, studi mengenai chain of custody menegaskan bahwa keabsahan bukti tidak hanya ditentukan oleh konten data, tetapi juga oleh kemampuan untuk menelusuri secara sistematis setiap tahapan pengelolaan bukti sejak akuisisi hingga presentasi di pengadilan [22]. Dalam konteks ini, ketiadaan pengaturan eksplisit mengenai audit teknis dan verifikasi independen dalam regulasi LI di Indonesia menunjukkan adanya kesenjangan antara standar forensik digital yang ideal dan praktik regulasi yang ada.

Dibandingkan dengan pendekatan dalam literatur sebelumnya yang umumnya menitikberatkan pada aspek prosedural forensik atau legalitas penyadapan secara terpisah, penelitian ini menunjukkan bahwa desain regulasi LI secara langsung mempengaruhi kualitas teknis bukti digital. Dengan kata lain, regulasi tidak hanya berfungsi sebagai instrumen legitimasi hukum, tetapi juga sebagai faktor determinan dalam menjaga integritas data dan keberlanjutan chain of custody dalam lingkungan digital yang kompleks [21][22].

Dengan demikian, kontribusi utama temuan ini adalah menunjukkan bahwa kelemahan regulasi, khususnya dalam aspek pengawasan dan standardisasi prosedur, dapat menciptakan risiko sistemik terhadap keandalan bukti digital. Hal ini memperluas pemahaman sebelumnya dengan menempatkan regulasi sebagai bagian integral dari ekosistem forensik digital, bukan sekadar kerangka normatif yang berdiri sendiri.

4.4. Diskusi: Implikasi Keamanan Siber dan Tata Kelola Lawful Interception

Dari perspektif keamanan siber, hasil penelitian ini menunjukkan bahwa desain regulasi Lawful Interception (LI) memiliki implikasi langsung terhadap tingkat keamanan sistem komunikasi digital. Praktik intersepsi yang memerlukan titik akses khusus (interception point) berpotensi memperluas attack surface apabila tidak disertai dengan kontrol keamanan yang memadai, sebagaimana yang dapat dilihat pada Gambar 2. Risiko ini mencakup kemungkinan akses tidak sah, kebocoran data hasil intersepsi, serta manipulasi data yang berdampak pada integritas bukti digital [20].

Gambar 2. Skema umum titik intersepsi komunikasi dalam praktik *Lawful Interception*

Temuan ini konsisten dengan konsep *attack surface* dalam keamanan sistem yang menyatakan bahwa setiap penambahan titik akses akan meningkatkan potensi eksploitasi jika tidak diimbangi dengan mekanisme kontrol yang kuat [20]. Selain itu, dalam literatur keamanan siber, desain sistem yang tidak mempertimbangkan prinsip pemisahan peran (*separation of duties*) dan *trust boundary* berpotensi menciptakan kerentanan struktural dalam pengelolaan sistem yang melibatkan data sensitif [18]. Dalam konteks penelitian ini, konsentrasi kewenangan dalam praktik LI di Indonesia menunjukkan adanya potensi pelanggaran prinsip-prinsip tersebut.

Lebih lanjut, dibandingkan dengan studi sebelumnya yang melihat LI sebagai instrumen penegakan hukum semata, penelitian ini menunjukkan bahwa regulasi LI juga harus dipahami sebagai bagian dari tata kelola keamanan siber nasional. Hal ini sejalan dengan pandangan bahwa tata kelola keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada desain kebijakan dan struktur kelembagaan yang mengatur penggunaan teknologi tersebut [23].

Temuan penelitian ini juga memperkuat argumen bahwa ketidakharmonisan antara kebutuhan intersepsi dan perlindungan keamanan komunikasi dapat menciptakan dilema struktural dalam sistem keamanan siber. Upaya memperluas kemampuan intersepsi tanpa penguatan regulasi dan pengawasan teknis yang memadai berpotensi menurunkan tingkat keamanan sistem komunikasi secara keseluruhan, sebagaimana diingatkan dalam literatur mengenai *privacy by design* dan *data protection* dalam sistem siber [24].

Dengan demikian, penelitian ini memberikan kontribusi dengan menunjukkan bahwa kelemahan regulasi LI tidak hanya berdampak pada aspek hukum, tetapi juga pada keamanan operasional sistem komunikasi dan perlindungan data sensitif. Integrasi antara regulasi yang jelas, mekanisme pengawasan yang kuat, dan penerapan prinsip keamanan siber menjadi prasyarat penting untuk memastikan bahwa LI dapat berfungsi secara efektif tanpa menciptakan kerentanan baru dalam sistem komunikasi digital.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa pengaturan *Lawful Interception* (LI) di Indonesia belum sepenuhnya selaras dengan karakteristik komunikasi digital modern dan prinsip keamanan siber. Secara umum, hasil analisis mengindikasikan bahwa sebagian besar regulasi masih bersifat terfragmentasi dan belum menyediakan mekanisme yang konsisten dalam aspek otorisasi, pengawasan, dan pengelolaan data hasil intersepsi. Kondisi ini berdampak pada munculnya variasi prosedural yang berpotensi melemahkan integritas bukti digital dalam praktik forensik siber.

Dari perspektif teknis, temuan penelitian menunjukkan bahwa mekanisme intersepsi dalam lingkungan komunikasi terenkripsi secara signifikan membatasi akses terhadap konten komunikasi, sehingga dalam banyak kasus hanya metadata yang dapat diperoleh. Selain itu, keberadaan titik intersepsi yang tidak diimbangi dengan kontrol keamanan yang memadai berpotensi memperluas *attack surface* sistem komunikasi dan meningkatkan risiko terhadap integritas data hasil intersepsi.

Lebih lanjut, hasil analisis secara konsisten menunjukkan bahwa belum adanya pengaturan eksplisit terkait audit teknis dan verifikasi independen menjadi faktor utama yang melemahkan jaminan keandalan bukti digital. Ketiadaan mekanisme tersebut meningkatkan potensi sengketa dalam proses pembuktian, khususnya pada kasus kejahatan siber yang kompleks dan bergantung pada validitas bukti digital.

Secara keseluruhan, penelitian ini menegaskan bahwa efektivitas LI tidak hanya ditentukan oleh legitimasi hukum, tetapi juga oleh kesesuaian desain regulasi dengan prinsip keamanan siber dan standar forensik digital. Oleh karena itu, diperlukan upaya harmonisasi regulasi yang secara sistematis mengintegrasikan aspek legal, teknis, dan tata kelola untuk memastikan bahwa LI dapat mendukung penegakan hukum siber tanpa menciptakan kerentanan baru dalam sistem komunikasi digital.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Laboratorium Rekayasa Perangkat Lunak Kriptografi Poltek Siber dan Sandi Negara, Sekolah Tinggi Ilmu Kepolisian, Pusat Studi Intelijen Keamanan STIK dan pihak-pihak yang telah memberikan masukan dalam penyusunan artikel ini.

REFERENSI

[1] M. Lowenthal, Intelligence: From Secrets to Policy, 8th ed. Washington, DC, USA: CQ Press, 2023.

[2] S. Landau, *Listening In: Cybersecurity in an Insecure Age*. New Haven, CT: Yale University Press, 2017.

[3] H. Abelson *et al.*, "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 69–79, 2015.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 4th ed. London, UK: Academic Press, 2020.

[5] Institute for Criminal Justice Reform (ICJR), Mengatur Ulang Penyadapan dalam Sistem Peradilan Pidana. Jakarta, Indonesia: ICJR, 2020.

[6] Mahkamah Konstitusi Republik Indonesia, Putusan Nomor 5/PUU-VIII/2010 tentang Pengujian Undang-Undang terhadap Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Jakarta, Indonesia, 2010.

[7] S. Brenner, *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger, 2010.

[8] J. Goldsmith, Power and Constraint: The Accountable Presidency After 9/11. New York, NY, USA: W. W. Norton & Company, 2012.

[9] D. A. Yuvens, R. S. Widigda, and A. Sharifa, "Dilema Upaya Hukum Terhadap Penyadapan," Jurnal Hukum & Pembangunan, vol. 47, no. 3, pp. 286–309, 2017, doi: 10.21143/jhp.vol47.no3.1578.

[10] S. Dewi, Cyber Law: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce. Bandung, Indonesia: Refika Aditama, 2011.

[11] W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 2007.

[12] G. Palmer, A Road Map for Digital Forensic Research. Utica, NY, USA: DFRWS, 2001.

[13] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," International Journal of Digital Evidence, vol. 2, no. 2, pp. 1–20, 2003.

[14] N. M. Richards, "The Dangers of Surveillance," *Harvard Law Review*, vol. 126, no. 7, pp. 1934-1965, 2013.

[15] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64-S73, 2010.

[16] P. M. Marzuki, Penelitian Hukum. Jakarta, Indonesia: Kencana, 2017.

[17] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[18] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva, Switzerland: ISO, 2022.

[19] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering. Indianapolis, IN, USA: Wiley, 2010.

[20] P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371-386, 2011.

[21] E. Casey, "Error, uncertainty, and loss in digital evidence," International Journal of Digital Evidence, vol. 1, no. 2, 2002.

[22] Y. Prayudi and A. N. Sn, "Digital Chain of Custody: State of The Art," International Journal of Computer Applications, vol. 114, no. 5, pp. 1–9, 2015, doi: 10.5120/19971-1856.

[23] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2013.

[24] A. Cavoukian, Privacy by Design: The 7 Foundational Principles — Implementation and Mapping of Fair Information Practices. Ontario, Canada: Information and Privacy Commissioner of Ontario, 2011.