Department of Digital Business
**Journal of Artificial Intelligence and Digital Business (RIGGS)**
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 3152-3159
P-ISSN: 2963-9298, e-ISSN: 2963-914X

# Anatomi Pengelolaan Data di Satintelkam Polres Karanganyar: Mengidentifikasi Celah Penyebaran Data dan Dampaknya terhadap Keamanan Konsumen

Antika Puji Setiyaningsih, Dimas Febryyano Hanivan, Ilham Sabilillah Yudatama, Jesika Anatasya, Prifka Cahyani
Ilmu Hukum, Fakultas Hukum, Universitas Slamet Riyadi
antikapujisetiya@gmail.com, dimashanivan@gmail.com, ilhamyudatamaa@gmail.com, jesikaanatasya25@gmail.com, prifkacahyani@gmail.com

***Abstrak***

*Penelitian ini bertujuan untuk mengevaluasi secara mendalam tata kelola data pada Satuan Intelijen dan Keamanan (Satintelkam) Polres Karanganyar dengan fokus pada identifikasi celah keamanan dalam proses distribusi informasi serta implikasinya terhadap perlindungan data masyarakat. Urgensi penelitian ini didasarkan pada meningkatnya risiko kerentanan data pribadi dalam birokrasi pelayanan publik kepolisian. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus. Pengumpulan data dilakukan melalui teknik wawancara mendalam terhadap enam personel Satintelkam, observasi langsung terhadap prosedur operasional standar, serta telaah dokumen kebijakan internal organisasi. Hasil penelitian mengungkapkan tiga celah krusial dalam sistem tata kelola data. Pertama, belum tersedianya protokol verifikasi formal terhadap identitas dan urgensi pihak penerima data sebelum proses distribusi dilakukan. Kedua, terdapat tumpang tindih wewenang antara fungsi intelijen murni dan fungsi pelayanan publik yang menyebabkan akses data menjadi tidak terotorisasi dengan ketat. Ketiga, sistem pencatatan digital yang ada belum mampu menghasilkan jejak audit (audit trail) yang akurat, sehingga penyebaran data tidak terdokumentasi secara sistematis. Celah-celah keamanan tersebut secara empiris berdampak pada potensi kebocoran informasi pribadi pelapor serta data transaksi sensitif kepada pihak ketiga yang tidak berwenang. Dampak lebih luas mencakup peningkatan risiko pencurian identitas, eksploitasi data untuk praktik ilegal, serta penurunan signifikansi kepercayaan publik terhadap profesionalisme institusi kepolisian. Sebagai solusi strategis, penelitian ini merekomendasikan implementasi sistem otorisasi akses berlapis (multi-level authorization) dan pelaksanaan audit keamanan informasi secara periodik guna memitigasi risiko penyalahgunaan data di masa depan.*

*Kata kunci:* *Tata Kelola Data, Satitelkam, Penyebaran Data, Kebocoran Data, Verifikasi Penerima Data*

## 1. Latar Belakang

Perkembangan teknologi digital telah mendorong terjadinya transformasi mendasar dalam tata kelola data di sektor pemerintahan, termasuk dalam tubuh institusi kepolisian. Perubahan ini tidak hanya berkaitan dengan penggunaan perangkat teknologi, tetapi juga menyangkut pergeseran paradigma dalam memandang data sebagai elemen strategis. Jika sebelumnya data lebih diposisikan sebagai dokumen administratif, maka dalam konteks saat ini data telah berkembang menjadi aset penting yang berperan dalam mendukung pengambilan keputusan, menjaga stabilitas keamanan, serta meningkatkan kualitas pelayanan publik. Oleh karena itu, tuntutan terhadap sistem pengelolaan data yang akurat, cepat, dan aman menjadi semakin tidak terelakkan. Integrasi teknologi informasi dalam sistem kepolisian bahkan turut membentuk model kerja baru yang menekankan pada aspek prediktif, responsif, dan akuntabel.

Dalam struktur organisasi kepolisian di tingkat daerah, Satuan Intelijen dan Keamanan (Satintelkam) memiliki posisi strategis sebagai unit yang bertanggung jawab terhadap pengelolaan data dan informasi. Peran tersebut mencakup proses pengumpulan, pengolahan, analisis, hingga distribusi data yang berkaitan dengan keamanan dan ketertiban masyarakat. Tidak hanya terbatas pada fungsi intelijen, Satintelkam juga berperan dalam pelayanan administratif kepada masyarakat, seperti penerbitan Surat Keterangan Catatan Kepolisian (SKCK), perizinan kegiatan, serta berbagai bentuk layanan lain yang melibatkan data pribadi warga. Dengan demikian, ruang lingkup

pengelolaan data di Satintelkam menjadi semakin luas dan kompleks, karena mencakup data strategis sekaligus data pribadi masyarakat yang bersifat sensitif.

Namun demikian, kompleksitas tersebut tidak selalu diimbangi dengan kesiapan sistem pengelolaan yang memadai. Dalam praktiknya, masih terdapat berbagai kendala yang menunjukkan adanya kelemahan dalam tata kelola data, seperti belum optimalnya integrasi sistem antarinstansi, keterbatasan infrastruktur teknologi, serta belum tersedianya mekanisme pertukaran data yang aman dan terstandarisasi secara nasional. Kondisi ini berpotensi menimbulkan fragmentasi data, duplikasi informasi, hingga celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Di sisi lain, meningkatnya volume dan variasi data juga memperbesar risiko kebocoran apabila tidak diiringi dengan sistem perlindungan yang kuat.

Kelemahan dalam pengelolaan data tidak hanya bersumber dari aspek teknologi, tetapi juga berkaitan erat dengan faktor organisasi dan sumber daya manusia. Belum optimalnya penerapan standar operasional prosedur, lemahnya sistem pengawasan internal, serta kurangnya penerapan kontrol akses berbasis kewenangan menjadi indikasi adanya permasalahan dalam tata kelola kelembagaan. Selain itu, tingkat literasi digital dan kesadaran personel terhadap pentingnya keamanan data juga menjadi faktor krusial yang memengaruhi efektivitas sistem. Dalam banyak kasus, kebocoran data justru terjadi akibat kelalaian manusia (human error) atau praktik kerja yang tidak sesuai dengan prinsip keamanan informasi.

Dampak dari kelemahan tersebut tidak hanya dirasakan oleh institusi, tetapi juga oleh masyarakat sebagai pemilik data. Kebocoran data pribadi dapat menimbulkan berbagai konsekuensi negatif, seperti penyalahgunaan identitas, penipuan berbasis data, pelanggaran privasi, hingga ancaman terhadap keamanan individu. Lebih jauh lagi, kondisi ini berpotensi menurunkan tingkat kepercayaan publik terhadap institusi kepolisian sebagai pengelola data. Kepercayaan publik merupakan elemen penting dalam legitimasi institusi penegak hukum, sehingga kegagalan dalam menjaga keamanan data dapat berdampak pada menurunnya kredibilitas dan akuntabilitas lembaga. Secara normatif, Indonesia telah memiliki landasan hukum yang mengatur perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022. Regulasi ini menegaskan kewajiban bagi setiap pengendali data, termasuk institusi pemerintah, untuk menjamin keamanan, kerahasiaan, serta penggunaan data secara sah dan terbatas. Namun, dalam implementasinya masih terdapat kesenjangan antara ketentuan normatif dengan praktik di lapangan. Faktor seperti lemahnya pengawasan, keterbatasan kapasitas sumber daya manusia, serta belum optimalnya penegakan hukum menjadi tantangan dalam mewujudkan perlindungan data yang efektif.

Berdasarkan uraian tersebut, terlihat adanya kesenjangan penelitian (research gap), khususnya terkait belum banyaknya kajian yang secara spesifik membahas pengelolaan data pada Satintelkam di tingkat Polres, terutama dalam konteks otonomi pengelolaan data dan identifikasi celah kerentanan pada setiap tahapan siklus data. Sebagian besar penelitian sebelumnya lebih berfokus pada aspek regulasi atau sistem secara makro, sehingga belum mampu menggambarkan kondisi operasional di tingkat unit kerja secara rinci. Oleh karena itu, penelitian ini menjadi relevan untuk mengisi kekosongan tersebut dengan memberikan analisis yang lebih mendalam dan kontekstual. Sejalan dengan hal tersebut, rumusan masalah dalam penelitian ini disusun untuk mengkaji secara komprehensif praktik pengelolaan data pada Satintelkam Polres Karanganyar. Fokus utama penelitian diarahkan pada bagaimana proses pengelolaan data dilaksanakan berdasarkan tahapan siklus informasi, yang meliputi pengumpulan, verifikasi, penyimpanan, distribusi, hingga pemusnahan data. Setiap tahapan dianalisis tidak hanya sebagai prosedur administratif, tetapi juga sebagai bagian dari sistem pengendalian yang menentukan kualitas serta tingkat keamanan informasi yang dikelola.

Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi berbagai bentuk kerentanan (vulnerability) yang muncul dalam setiap tahapan tersebut, dengan mempertimbangkan faktor-faktor penyebabnya yang meliputi aspek teknologi, tata kelola organisasi, dan kapasitas sumber daya manusia. Lebih lanjut, penelitian ini mengkaji tingkat kesesuaian antara praktik pengelolaan data yang dilakukan dengan ketentuan hukum yang berlaku, khususnya Undang-Undang Perlindungan Data Pribadi, guna menilai sejauh mana prinsip-prinsip perlindungan data telah diterapkan secara efektif. Pada akhirnya, penelitian ini diarahkan untuk menganalisis implikasi dari kelemahan pengelolaan data terhadap perlindungan data pribadi masyarakat serta tingkat kepercayaan publik terhadap institusi kepolisian. Dengan demikian, rumusan masalah dalam penelitian ini dirancang secara komprehensif dengan mencakup dimensi teknis, kelembagaan, hukum, dan sosial, sehingga diharapkan dapat memberikan kontribusi dalam perumusan strategi penguatan sistem pengelolaan data yang lebih aman, akuntabel, dan sesuai dengan prinsip tata kelola yang baik.

DOI: https://doi.org/10.31004/riggs.v5i2.8631

## 2. Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan desain naratif untuk memahami secara mendalam proses pengelolaan data serta celah penyebaran informasi di Satintelkam Polres Karanganyar dan dampaknya terhadap keamanan konsumen. Metode ini dipilih karena mampu menggali pengalaman, praktik, dan alur kerja berdasarkan perspektif informan secara kontekstual dan menyeluruh. Data penelitian terdiri dari data primer. Data primer diperoleh melalui wawancara mendalam dengan personel yang terlibat dalam pengelolaan data serta observasi non-partisipatif terhadap proses pengelolaan data di lapangan. Teknik pengumpulan data dilakukan secara terpadu melalui wawancara semi-terstruktur, observasi, dan dokumentasi guna memastikan kelengkapan dan keakuratan informasi.

Analisis data dilakukan secara kualitatif naratif melalui tahapan reduksi, kategorisasi, dan interpretasi data. Penelitian ini mengidentifikasi pola pengelolaan data, titik rawan penyebaran, serta faktor penyebab dan dampaknya terhadap keamanan konsumen. Validitas data dijaga melalui triangulasi sumber dan metode, sedangkan kesimpulan ditarik secara induktif untuk memberikan gambaran komprehensif mengenai celah pengelolaan data dan implikasinya dalam konteks kelembagaan.

## 3. Hasil dan Diskusi

Pengelolaan data di satuan intelijen keamanan (satintelkam) polres karanganyar pada dasarnya telah mengikuti tahapan umum dalam siklus pengelolaan informasi, yang meliputi proses pengumpulan, verifikasi, penyimpanan, dan distribusi data. tahapan ini sejalan dengan konsep data *lifecycle* yang dikemukakan oleh khatri dan brown (2010), yang menekankan bahwa pengelolaan data mencakup serangkaian proses terstruktur dari perolehan hingga pemanfaatan data. Berdasarkan temuan di lapangan, proses pengumpulan data dilakukan melalui dua metode utama, yaitu secara langsung melalui kegiatan lapangan serta secara tidak langsung melalui sumber-sumber digital. Data yang diperoleh kemudian melalui tahap verifikasi sebelum disimpan dalam bentuk arsip fisik maupun database digital internal.

Dalam aspek penyimpanan, sistem yang digunakan masih bersifat kombinatif antara metode konvensional dan digital. hal ini menunjukkan adanya upaya adaptasi terhadap perkembangan teknologi, namun belum sepenuhnya didukung oleh sistem keamanan informasi yang terintegrasi. menurut Laudon dan Laudon (2016), sistem informasi yang efektif tidak hanya ditentukan oleh kemampuan penyimpanan data, tetapi juga oleh aspek keamanan dan kontrol yang menyertainya. Distribusi data dilakukan secara terbatas berdasarkan tingkat kewenangan, tetapi dalam praktiknya masih ditemukan penggunaan media komunikasi non-resmi untuk mempercepat arus informasi antar personel.

Temuan penelitian menunjukkan adanya beberapa celah dalam pengelolaan data, terutama pada tahap distribusi dan pengamanan informasi. penggunaan media komunikasi umum yang tidak memiliki sistem enkripsi khusus menjadi salah satu potensi risiko kebocoran data. selain itu, belum optimalnya penerapan pembatasan akses berbasis peran *(role-based access control)* memungkinkan adanya akses data oleh pihak yang tidak memiliki otoritas penuh. hal ini sejalan dengan temuan Solove (2008) yang menyatakan bahwa kebocoran data seringkali tidak hanya disebabkan oleh kelemahan teknologi, tetapi juga oleh kegagalan dalam pengaturan akses dan pengawasan.

Apabila dianalisis menggunakan kerangka keamanan informasi, kondisi tersebut menunjukkan bahwa prinsip kerahasiaan *(confidentiality)* belum sepenuhnya terpenuhi. Dalam konsep CIA triad yang dikemukakan oleh Whitman dan Mattord (2011), keamanan informasi bertumpu pada tiga pilar utama, yaitu kerahasiaan, integritas, dan ketersediaan. Kelemahan pada salah satu aspek tersebut dapat berdampak pada keseluruhan sistem keamanan informasi. Di sisi lain, potensi gangguan terhadap integritas (*integrity*) dan ketersediaan (*availability*) data juga dapat muncul apabila sistem pengelolaan tidak diperkuat secara menyeluruh. Faktor sumber daya manusia, seperti kurangnya kesadaran terhadap pentingnya keamanan data dan potensi terjadinya human error, juga menjadi variabel penting sebagaimana dikemukakan oleh Schneier (2015) bahwa manusia seringkali menjadi titik terlemah dalam sistem keamanan.

Dari perspektif yuridis, kondisi tersebut juga belum sepenuhnya selaras dengan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. dalam pasal 20 ditegaskan bahwa pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi dari pemrosesan yang tidak sah. selain itu, pasal

DOI: https://doi.org/10.31004/riggs.v5i2.8631

35 menekankan kewajiban untuk mencegah akses tidak sah terhadap data pribadi yang dikelola. Penggunaan media komunikasi non-resmi serta lemahnya kontrol akses sebagaimana ditemukan dalam penelitian ini menunjukkan adanya potensi ketidaksesuaian dengan prinsip-prinsip perlindungan data yang diatur dalam undang-undang tersebut.

Celah dalam pengelolaan data ini berimplikasi langsung terhadap keamanan konsumen, terutama dalam konteks perlindungan data pribadi dan informasi sensitif. menurut Westin (1967), privasi merupakan hak individu untuk mengontrol informasi tentang dirinya, sehingga kebocoran data dapat dikategorikan sebagai pelanggaran terhadap hak tersebut. dalam konteks hukum nasional, pelanggaran terhadap perlindungan data pribadi juga dapat menimbulkan konsekuensi hukum bagi institusi pengelola data, sebagaimana diatur dalam undang-undang perlindungan data pribadi. Kebocoran data berpotensi menimbulkan berbagai dampak negatif, seperti penyalahgunaan informasi, tindak penipuan, hingga pelanggaran privasi. Lebih lanjut, kondisi ini juga dapat menurunkan tingkat kepercayaan masyarakat terhadap institusi penegak hukum sebagai pengelola data publik, sebagaimana ditegaskan oleh Mayer, Davis, dan Schoorman (1995) bahwa kepercayaan publik sangat dipengaruhi oleh kemampuan institusi dalam menjaga integritas dan keamanan informasi.

Oleh karena itu, dapat disimpulkan bahwa permasalahan dalam pengelolaan data di satintelkam polres karanganyar tidak hanya terletak pada aspek teknis, tetapi juga pada tata kelola organisasi dan kesadaran sumber daya manusia. Diperlukan penguatan sistem keamanan informasi yang lebih terintegrasi, disertai dengan peningkatan kapasitas personel dalam memahami pentingnya perlindungan data, guna meminimalisasi risiko kebocoran serta menjaga keamanan konsumen secara lebih optimal, sekaligus memastikan kesesuaian dengan regulasi yang berlaku. Berikut merupakan tahap analisis:

**Analisis tahap pengumpulan data**

Secara normatif, praktik pengumpulan data di satintelkam telah mencerminkan keragaman sumber, yakni melalui metode langsung dan tidak langsung. Namun demikian, temuan ini justru mengindikasikan belum adanya standar operasional prosedur (SOP) yang terintegrasi dalam menjamin kualitas dan konsistensi data. Keberagaman sumber tanpa mekanisme kontrol yang ketat berpotensi menghasilkan data yang bias, redundan, atau bahkan tidak relevan. Dalam konteks ini, pengelolaan data belum sepenuhnya mencerminkan prinsip data governance yang menekankan standardisasi dan akuntabilitas (Khatri & Brown, 2010).

**Analisis tahap verifikasi data**

Meskipun proses verifikasi telah dilakukan, ketiadaan sistem verifikasi yang terdokumentasi dan terstandarisasi menunjukkan adanya kelemahan struktural dalam menjamin validitas data. Verifikasi yang bersifat situasional dan bergantung pada subjektivitas individu berpotensi menurunkan reliabilitas informasi. Kondisi ini mengindikasikan bahwa fungsi verifikasi belum berperan sebagai mekanisme kontrol kualitas, melainkan hanya sebagai prosedur administratif. Padahal, sebagaimana dikemukakan Laudon (2016), kualitas output sistem informasi sangat ditentukan oleh ketepatan dan konsistensi proses validasi data.

**Analisis tahap penyimpanan data**

Penggunaan sistem penyimpanan hibrida (fisik dan digital) tidak hanya mencerminkan fase transisi digital, tetapi juga menunjukkan belum matangnya strategi integrasi sistem informasi. Kondisi ini membuka dua lapis kerentanan sekaligus, yakni risiko kehilangan atau kerusakan data fisik, serta potensi kebocoran pada sistem digital yang tidak dilengkapi dengan pengamanan memadai. Lebih jauh, ketiadaan mekanisme keamanan seperti enkripsi, audit log, atau sistem pencadangan (backup) mengindikasikan bahwa perlindungan data belum menjadi prioritas strategis. Hal ini bertentangan dengan prinsip dasar keamanan informasi yang menuntut perlindungan menyeluruh terhadap aset data.

**Analisis tahap distribusi data**

Tahap distribusi merupakan titik paling problematis dalam keseluruhan sistem pengelolaan data. Penggunaan media komunikasi non-resmi untuk penyebaran informasi sensitif tidak hanya menunjukkan kelemahan teknis, tetapi juga mencerminkan rendahnya kesadaran institusional terhadap risiko keamanan data. praktik ini secara langsung melanggar prinsip kerahasiaan *(confidentiality*) dalam kerangka CIA triad (Whitman & Mattord, 2011).

DOI: https://doi.org/10.31004/riggs.v5i2.8631

lebih dari itu, normalisasi penggunaan saluran informal menunjukkan adanya budaya organisasi yang permisif terhadap pelanggaran prosedur, yang dalam jangka panjang berpotensi melemahkan sistem keamanan secara keseluruhan.

**Analisis celah pengelolaan data *(vulnerability)***

Celah yang ditemukan tidak dapat dipahami sebagai permasalahan parsial, melainkan sebagai indikasi kegagalan sistemik dalam tata kelola data. lemahnya kontrol akses, penggunaan media tidak aman, serta dominannya faktor human error menunjukkan bahwa sistem belum dibangun berdasarkan prinsip information *governance* yang komprehensif. Sebagaimana dikemukakan Solove (2008), kebocoran data seringkali merupakan hasil dari kegagalan struktural dalam mengatur akses dan tanggung jawab, bukan semata-mata kesalahan teknis. dengan demikian, permasalahan yang terjadi lebih tepat dipahami sebagai kegagalan tata kelola daripada sekadar keterbatasan teknologi.

**Analisis kesesuaian dengan UU perlindungan data pribadi**

Jika ditinjau secara yuridis, praktik pengelolaan data yang ditemukan menunjukkan adanya potensi ketidaksesuaian dengan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi. Kewajiban pengendali data untuk menjamin keamanan dan mencegah akses tidak sah sebagaimana diatur dalam pasal 20 dan pasal 35 belum sepenuhnya terimplementasi dalam praktik. penggunaan media komunikasi non-resmi dan lemahnya sistem kontrol akses dapat dikategorikan sebagai bentuk kelalaian dalam memenuhi kewajiban perlindungan data. Dalam konteks ini, permasalahan tidak hanya bersifat teknis, tetapi juga berpotensi menimbulkan konsekuensi hukum bagi institusi.

**Analisis dampak terhadap keamanan konsumen**

Implikasi dari celah pengelolaan data ini tidak berhenti pada ranah internal institusi, tetapi meluas hingga pada aspek keamanan konsumen. Kebocoran data pribadi berpotensi menyebabkan kerugian nyata bagi individu, mulai dari penyalahgunaan identitas hingga tindak kejahatan berbasis data. kondisi ini bertentangan dengan konsep privasi sebagai hak fundamental individu (Westin, 1967). Selain itu, kegagalan dalam melindungi data juga berdampak pada erosi kepercayaan publik terhadap institusi penegak hukum. sebagaimana dijelaskan Mayer et al. (1995), kepercayaan dibangun atas dasar kompetensi dan integritas, yang dalam konteks ini tercermin dari kemampuan menjaga keamanan informasi.

Secara keseluruhan, temuan penelitian ini menunjukkan bahwa permasalahan dalam pengelolaan data di satintelkam polres Karanganyar bukan sekadar persoalan teknis operasional, melainkan mencerminkan kelemahan mendasar dalam tata kelola, budaya organisasi, dan kepatuhan terhadap regulasi. Tanpa adanya intervensi yang sistematis dan komprehensif, celah yang ada akan terus berulang dan berpotensi menimbulkan risiko yang lebih besar, baik secara institusional maupun bagi masyarakat sebagai pengguna data.

Hasil analisis menunjukkan bahwa anatomi pengelolaan data di Satintelkam Polres Karanganyar pada dasarnya dapat dipahami sebagai rangkaian kerja yang saling berhubungan, mulai dari pengumpulan, penyimpanan, distribusi atau akses, hingga pemusnahan data. Setiap tahap memiliki fungsi strategis yang menentukan tingkat keamanan informasi, sekaligus menjadi titik rawan apabila pengendalian internal tidak dirancang secara ketat. Dalam konteks ini, pengelolaan data tidak hanya berhubungan dengan administrasi teknis, melainkan juga dengan perlindungan hukum atas data yang dikelola negara. Tata kelola data sangat penting untuk meningkatkan kualitas data dan menjamin kepatuhan hukum (Aqilla & Nasution, 2025). Pada tahap pengumpulan data, Satintelkam berperan sebagai unit yang menerima, menampung, dan mengolah berbagai informasi yang berkaitan dengan kepentingan keamanan, pelayanan publik, maupun kebutuhan administratif tertentu. Dalam praktiknya, pengumpulan data dapat bersumber dari permohonan masyarakat, kegiatan intelijen, verifikasi identitas, maupun dokumen pendukung lain yang melekat pada layanan kepolisian. Tahap ini sangat menentukan karena kualitas data pada awal proses akan memengaruhi kualitas keputusan pada tahap berikutnya. Akan tetapi, hasil analisis mengindikasikan bahwa celah sering muncul sejak tahap paling awal, terutama ketika prinsip pembatasan tujuan belum sepenuhnya diterapkan secara konsisten. Penelitian terdahulu menunjukkan bahwa tata kelola data publik digital di Indonesia masih menghadapi hambatan berupa keterbatasan infrastruktur, kesenjangan akses informasi, serta tumpang tindih regulasi antarinstansi (Muhamad Valery et al., 2025).

DOI: https://doi.org/10.31004/riggs.v5i2.8631

Pada tahap penyimpanan, data yang telah dihimpun idealnya ditempatkan dalam sistem yang aman, terklasifikasi, dan terlacak. Namun, analisis menunjukkan bahwa penyimpanan data merupakan salah satu titik paling rentan terhadap kebocoran apabila pengamanan fisik dan digital tidak berjalan beriringan. Celah struktural terlihat ketika pengelolaan data masih bergantung pada kebiasaan kerja individu, bukan pada sistem yang terstandardisasi. Dalam beberapa konteks lembaga publik, data sering tersebar dalam berkas fisik, perangkat lokal, atau folder digital yang hanya diketahui oleh petugas tertentu. Kondisi tersebut meningkatkan risiko akses tidak sah, kehilangan jejak audit, dan sulitnya penelusuran sumber kebocoran bila terjadi insiden. Data yang dikendalikan pemerintah seringkali sensitif (Purnama, 2025). Sifat sensitif tersebut menuntut tingkat kehati-hatian yang lebih tinggi dibandingkan pengelolaan dokumen administratif biasa, karena setiap data yang bocor dapat berimplikasi pada privasi individu, keamanan sosial, bahkan penyalahgunaan identitas.

Dari sisi teknologis, kelemahan yang paling menonjol adalah belum meratanya penerapan perlindungan data berbasis sistem. Dalam banyak organisasi publik, celah teknologis biasanya muncul dalam bentuk enkripsi yang belum memadai, pengaturan akses yang masih longgar, minimnya pencatatan aktivitas pengguna, atau tidak optimalnya pembaruan sistem. Hasil studi menunjukkan bahwa penerapan data governance berperan penting dalam kepatuhan hukum dan perlindungan data, meskipun masih terkendala oleh rendahnya literasi data dan adaptasi teknologi (Aqilla & Nasution, 2025). Temuan ini memperkuat dugaan bahwa kelemahan penyimpanan tidak semata-mata disebabkan oleh perangkat yang digunakan, tetapi juga oleh kemampuan aparatur dalam mengoperasikan sistem secara aman. Apabila petugas belum memiliki pemahaman memadai mengenai klasifikasi data, kata sandi yang kuat, otorisasi berlapis, dan prosedur cadangan data, maka penyimpanan yang tampak rapi secara administratif tetap rentan secara substansial.

Tahap distribusi atau akses merupakan bagian yang sangat menentukan karena pada tahap inilah data berpindah dari ruang penyimpanan menuju pihak yang membutuhkan. Dalam lingkungan Satintelkam, akses data dapat terjadi antarpetugas, antarfungsi, atau dengan satuan kerja lain sesuai kebutuhan tugas. Namun, semakin luas akses yang diberikan, semakin besar pula potensi penyebaran data apabila kontrolnya tidak ketat. Hasil analisis mengindikasikan bahwa celah distribusi sering muncul dalam bentuk akses yang terlalu bergantung pada relasi kerja informal, bukan pada prinsip kebutuhan untuk mengetahui (*need-to-know basis*). Situasi ini membuka peluang terjadinya penyalahgunaan wewenang, penggandaan data tanpa izin, atau pengiriman dokumen melalui sarana komunikasi yang kurang aman. Dalam konteks yang lebih luas, persoalan ini berkelindan dengan kondisi sistem informasi kepolisian di Indonesia yang masih belum terintegrasi antar satuan kerja, sehingga menghambat efektivitas pengelolaan data dan pelayanan publik berbasis digital (Hutapea, 2023). Ketidakterintegrasian tersebut dapat memperbesar kemungkinan duplikasi data, pertukaran data yang tidak terlacak, serta ketidakselarasan antara basis data satu unit dengan unit lainnya.

Secara kultural, celah distribusi juga dipengaruhi oleh kebiasaan kerja yang menempatkan kecepatan layanan di atas kehati-hatian terhadap data. Dalam organisasi yang berorientasi pada target layanan dan ketertiban operasional, ada kecenderungan data dianggap sebagai alat bantu kerja, bukan sebagai aset hukum yang harus dijaga kerahasiaannya secara ketat. Karena itu, kebocoran sering tidak muncul melalui tindakan kriminal yang besar, tetapi melalui tindakan kecil yang tampak sepele, seperti berbagi dokumen melalui perangkat pribadi, meninggalkan file terbuka, atau menyalin data ke media penyimpanan portabel tanpa pengamanan. Celah kultural seperti ini menjadi berbahaya ketika belum dibarengi dengan budaya kepatuhan dan pengawasan internal yang tegas. Di sinilah pentingnya etika organisasi, sebab perlindungan data bukan semata persoalan perangkat, melainkan juga soal kebiasaan kerja yang disiplin dan bertanggung jawab.

Tahap pemusnahan data sering kali menjadi tahap yang paling diabaikan, padahal justru di sini banyak risiko sisa data muncul. Data yang seharusnya telah dimusnahkan dapat tetap tertinggal dalam arsip, perangkat keras lama, cadangan digital, atau salinan yang tersebar di beberapa tempat. Bila pemusnahan tidak dilakukan dengan prosedur yang jelas, data lama dapat dipulihkan kembali dan menjadi sumber kebocoran baru. Hasil analisis menunjukkan bahwa kelemahan pada tahap ini lebih bersifat struktural dan prosedural. Banyak institusi publik cenderung fokus pada pengumpulan dan penyimpanan, tetapi belum memberikan perhatian yang seimbang pada siklus akhir data. Padahal, tata kelola yang baik menuntut siklus hidup data yang utuh, termasuk kapan data harus dihapus, bagaimana data dimusnahkan, dan siapa yang bertanggung jawab atas verifikasinya. Dalam keamanan data publik, pengendalian siklus hidup data menjadi penting karena data pemerintah bersifat sensitif dan berisiko disalahgunakan jika tidak dilindungi secara hukum dan teknis (Purnama, 2025).

DOI: https://doi.org/10.31004/riggs.v5i2.8631

Dari keseluruhan tahapan tersebut, temuan empiris atau indikatif menunjukkan bahwa potensi kebocoran data di Satintelkam dapat terjadi karena kombinasi beberapa faktor sekaligus. Pertama, adanya fragmentasi sistem dan belum optimalnya integrasi data antarunit sebagaimana juga ditemukan dalam sistem informasi kepolisian yang belum terintegrasi (Hutapea, 2023). Kedua, keterbatasan literasi data dan adaptasi teknologi yang membuat prosedur keamanan belum sepenuhnya dipahami dan dijalankan oleh semua personel (Aqilla & Nasution, 2025). Ketiga, faktor manusia yang tetap menjadi ancaman dominan, karena ancaman utama berasal dari kerentanan sistem dan faktor manusia (Bua & Idris, 2024). Temuan ini penting karena menunjukkan bahwa kebocoran data bukanlah peristiwa tunggal, melainkan hasil akumulasi kelemahan pada berbagai titik pengelolaan. Dengan kata lain, kebocoran bukan hanya soal "siapa membocorkan", tetapi juga soal "bagaimana sistem memungkinkan kebocoran itu terjadi".

Kelemahan sistem pengawasan internal juga terlihat pada belum kuatnya mekanisme kontrol berlapis terhadap akses, distribusi, dan pemusnahan data. Pengawasan internal idealnya mencakup pencatatan akses, audit berkala, pemisahan kewenangan, dan evaluasi kepatuhan terhadap SOP. Namun, apabila pengawasan masih bertumpu pada kepercayaan personal dan pemeriksaan administratif sesekali, maka pelanggaran kecil dapat luput dari deteksi. Dalam penelitian tentang keamanan data publik disebutkan bahwa keamanan sistem informasi publik memerlukan pengelolaan yang ketat karena data pemerintah bersifat sensitif dan berisiko disalahgunakan jika tidak dilindungi secara hukum dan teknis (Purnama, 2025). Pernyataan ini menegaskan bahwa pengawasan internal tidak boleh dipahami sebagai fungsi pelengkap, melainkan sebagai inti dari tata kelola data. Tanpa sistem pengawasan yang kuat, data yang telah dikumpulkan dengan sah tetap dapat berubah menjadi sumber risiko bagi keamanan konsumen atau masyarakat sebagai subjek data.

## 4. Kesimpulan

Penelitian ini menyimpulkan bahwa pengelolaan data di Satintelkam Polres Karanganyar masih memiliki celah kerentanan yang signifikan pada setiap tahapan siklus data, terutama pada fase distribusi dan penyimpanan. Fakta di lapangan menunjukkan bahwa penggunaan media komunikasi non-resmi dan belum optimalnya sistem otorisasi berlapis menjadi faktor utama yang memperbesar risiko kebocoran data pribadi masyarakat. Celah ini tidak hanya disebabkan oleh keterbatasan infrastruktur teknologi, tetapi juga berakar pada budaya organisasi yang cenderung mendahului kecepatan layanan daripada aspek keamanan data serta literasi digital personel yang belum merata. Implikasi dari kondisi ini adalah munculnya potensi ancaman terhadap privasi konsumen, risiko penyalahgunaan identitas, serta degradasi kepercayaan publik terhadap kredibilitas institusi kepolisian sebagai pengelola data sensitif. Secara spekulatif, jika perbaikan sistemik tidak segera dilakukan melalui standarisasi SOP yang selaras dengan Undang-Undang Perlindungan Data Pribadi dan penguatan audit internal, maka kerentanan ini dapat berkembang menjadi krisis akuntabilitas hukum bagi institusi. Oleh karena itu, disarankan bagi penelitian selanjutnya untuk mengkaji efektivitas penerapan sistem *blockchain* atau teknologi enkripsi mutakhir dalam mengamankan pertukaran data intelijen di tingkat kepolisian resort guna menjamin integritas informasi secara lebih transparan dan terlacak.

## Referensi

[1] Aqilla, N. P., & Nasution, M. I. P. (2025). Peran data governance dalam keamanan dan privasi data di era digital. Jurnal Multidisiplin Ilmu Akademik, 2(3).
[2] Bua, I. T., & Idris, N. I. (2024). Analisis kebijakan keamanan siber di Indonesia: Studi kasus kebocoran data nasional pada tahun 2024. Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, 2(2).
[3] Hutapea, G. T. R. (2023). Penyatuan sistem informasi kepolisian yang terintegrasi untuk mewujudkan big data Polri guna peningkatan kualitas pelayanan publik. Jurnal Ilmu Kepolisian, 17(1). https://www.jurnalptik.id/index.php/JIK/article/view/380
[4] Muhamad Valery, Aranta, B. A., Lawaty, L., & Utama, C. (2025). Penerapan prinsip keterbukaan, keadilan, dan kepastian hukum dalam tata kelola data publik digital di Indonesia. J-CEKI: Jurnal Cendekia Ilmiah, 5(1), 3029–3040.
[5] Purnama, I. K. A. (2025). Keamanan data publik: Strategi perlindungan dalam infrastruktur digital pemerintahan. Jurnal Hukum Mimbar Justitia, 11(1).
[6] Vitaloka, I. D., Dewi, A. A. S. L., & Suryani, L. P. (2023). Pertanggungjawaban kepolisian sebagai penyidik dalam tindak pidana narkotika. Jurnal Konstruksi Hukum, 4(3), 348–353.
[7] Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1)
[8] Laudon, K. C., & Laudon, J. P. (2016). Management Information Systems: Managing the Digital Firm (14th ed.).
[9] Solove, D. J. (2008). Understanding Privacy. Harvard University Press. Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security (4th ed.).
[10] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
[11] Westin, A. F. (1967). Privacy and Freedom. Atheneum.
[12] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3)

DOI: https://doi.org/10.31004/riggs.v5i2.8631

[13] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2010). The human aspects of information security questionnaire. Computers & Security, 29(8)
[14] Schultz, E. E. (2005). The human factor in security. Computers & Security, 24(6)
[15] Wang, H., & Wang, S. (2010). A review of data breach notification laws. Journal of Information Privacy and Security, 6(3)
[16] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4)
[17] Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59(2)
[18] Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. Information Systems Management, 29(4)
[19] Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2)
[20] Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. Government Information Quarterly, 27(4)

DOI: https://doi.org/10.31004/riggs.v5i2.8631