

PENERAPAN ANALITIK AUDIO DAN PEMINDAI BIOMETRIK SEBAGAI SISTEM PERINGATAN DINI PENGAMANAN LAPAS DAN RUTAN

Ananda Fabiyan Nasrullah

Program Studi Manajemen Pemasyarakatan, Politeknik

Imigrasi dan Pemasyarakatan Indonesia

DOI. <https://doi.org/10.52472/jcm.v3i1.774>

Journal of Correctional Management
2026, Vol.3 (1) 1 - 10
Politeknik Ilmu Pemasyarakatan

Review
23-05-2026

Accepted
25-06-2026

Abstract

Overcrowding, complex inmate movement, and limited staff attention increase the need for earlier and more accountable security detection in prisons and detention centers. This article formulates a human-supervised early-warning model that integrates audio analytics and biometric verification through a directed narrative review of correctional regulations, official reports, technical standards, and recent correctional surveillance research. Audio analytics is positioned as an anomaly-alert mechanism rather than proof of aggression, while biometrics supports one-to-one identity verification at controlled access points. The proposed workflow connects sensor alerts, human verification, graded response, incident recording, and periodic evaluation. Findings emphasize that technology cannot replace dynamic security, professional judgment, or direct officer-inmate interaction. Implementation requires site mapping, representative performance testing, privacy-by-design, access controls, fallback procedures, audit trails, and independent review of false alerts and demographic differentials. A phased pilot is recommended because empirical evidence on audio analytics in correctional settings remains limited and has documented nuisance and false alerts. Effectiveness should be measured through response time, verified detection, operational continuity, fairness, privacy incidents, and staff workload.

Keywords: audio analytics; biometrics; correctional security; early warning; smart prison

Abstrak

Kepadatan hunian, kompleksitas pergerakan warga binaan, dan keterbatasan perhatian petugas meningkatkan kebutuhan deteksi keamanan yang lebih dini serta akuntabel di lapas dan rutan. Artikel ini merumuskan model peringatan dini dengan pengawasan manusia yang mengintegrasikan analitik audio dan verifikasi biometrik melalui studi kepustakaan naratif-terarah terhadap regulasi pemasyarakatan, laporan resmi, standar teknis, dan penelitian mutakhir mengenai surveilans koreksional. Analitik audio ditempatkan sebagai pemicu pemeriksaan anomali, bukan bukti terjadinya agresi, sedangkan biometrik mendukung verifikasi identitas satu-band-ing-satu pada titik akses terkendali. Alur yang diusulkan menghubungkan peringatan sensor, verifikasi petugas, respons berjenjang, pencatatan insiden, dan evaluasi berkala. Teknologi tidak menggantikan keamanan dinamis, pertimbangan profesional, atau interaksi langsung petugas dengan warga binaan. Implementasi memerlukan pemetaan lokasi, pengujian kinerja yang representatif, perlindungan data sejak desain, pembatasan akses, prosedur cadangan, jejak audit, serta peninjauan independen atas peringatan palsu dan perbedaan kinerja antarkelompok. Uji coba bertahap diperlukan karena bukti empiris analitik audio di lingkungan koreksional masih terbatas. Efektivitas diukur melalui waktu respons, deteksi terverifikasi, kesinambungan operasi, keadilan, insiden privasi, dan beban kerja petugas.

Kata kunci: analitik audio; biometrik; keamanan pemasyarakatan; peringatan dini; penjara cerdas

Pendahuluan

Pengamanan merupakan salah satu fungsi utama sistem pemasyarakatan Indonesia. Undang-Undang Republik Indonesia Nomor 22 Tahun 2022 menempatkan pengamanan bersama pelayanan, pembinaan, pembimbingan ke-masyarakatan, perawatan, dan pengamanan dalam satu sistem perlakuan yang menghormati hak asasi manusia. Pengamanan karena itu tidak hanya bertujuan menjaga tembok, pintu, dan ketertiban, tetapi juga menciptakan kondisi aman agar layanan serta pembinaan dapat berlangsung. Keamanan yang efektif perlu mencegah kekerasan, pelarian, penyelundupan, penyamaran identitas, dan gangguan lain tanpa menghilangkan martabat warga binaan maupun mengubah lembaga menjadi ruang pengawasan yang tidak terkendali.

Tantangan tersebut menjadi lebih berat dalam kondisi kelebihan kepadatan. Kementerian Imigrasi dan Pemasyarakatan melaporkan bahwa pada April 2026 terdapat 271.468 penghuni pada kapasitas ideal 146.860 orang, atau tingkat kelebihan kepadatan sekitar 85 persen. Kepadatan tidak tersebar merata, tetapi angka nasional tersebut menunjukkan besarnya tekanan terhadap ruang hunian, pergerakan, layanan, dan pengawasan. Pada lingkungan yang padat, petugas harus memantau banyak interaksi secara bersamaan, mengatur perpindahan warga binaan ke klinik, tempat ibadah, ruang kunjungan, kegiatan pembinaan, dan area kerja, serta tetap menyelesaikan pencatatan administratif. Gangguan kecil dapat berkembang cepat ketika ruang terbatas dan ketegangan meningkat.

Pengamanan konvensional mengan-dalkan kontrol akses, pemeriksaan fisik, apel, patroli, kamera, laporan, serta

pengetahuan petugas mengenai situasi blok. Unsur tersebut tetap penting, tetapi memiliki keterbatasan. Kamera tidak selalu dipantau setiap saat; terdapat titik buta; suara tidak tertangkap oleh pengamanan visual; dan verifikasi identitas manual dapat melambat pada arus pergerakan yang padat. Kelelahan, gangguan perhatian, pergantian regu, kualitas komunikasi, serta beban administrasi juga memengaruhi konsistensi respons. Per-soalannya bukan bahwa petugas tidak bekerja, melainkan kapasitas perhatian manusia memiliki batas sehingga dibutuhkan alat bantu yang memperluas kesadaran situasional.

Analitik audio dan pemindai biometrik menawarkan dua fungsi berbeda. Analitik audio mengolah karakteristik sinyal untuk menandai pola yang diperkirakan berkaitan dengan teriakan, ketakutan, benturan, atau agresi verbal, kemudian mengirim peringatan untuk diverifikasi. Pemindai biometrik mem-bandingkan karakteristik biologis, terutama wajah atau sidik jari, dengan templat identitas yang telah terdaftar. Dalam pengamanan lapas/rutan, analitik audio berpotensi mempercepat penemuan anomali, sedangkan biometrik berpotensi memperkuat kepastian identitas pada pintu tertentu. Keduanya bukan teknologi yang sama dan tidak boleh digabungkan dalam satu klaim efektivitas yang berlebihan.

Pengalaman internasional memperli-hatkan peluang sekaligus peringatan. Singapore Prison Service pada 2025 mengu-mumkan uji coba sistem kunjungan jarak jauh otonom yang memakai pengenalan wajah, kecerdasan buatan, dan analisis sentimen untuk verifikasi pengunjung serta pemicu peringatan. Namun, pengu-muman uji coba bukan bukti bahwa teknologi selalu akurat pada seluruh konteks. Evaluasi Peterson et al. (2024) pada

dua penjara negara bagian Minnesota menemukan bukti terbatas bahwa peningkatan surveilans menurunkan pelanggaran. Penempatan kamera baru membantu investigasi, tetapi seluruh peringatan analitik audio selama periode penelitian merupakan peringatan gangguan atau peringatan palsu, bukan deteksi pertarungan sebagaimana dimaksud. Temuan ini menuntut pendekatan yang lebih kritis daripada sekadar menyebut teknologi sebagai solusi otomatis.

Artikel ini menjawab empat pertanyaan: bagaimana posisi analitik audio dan biometrik dalam keamanan dinamis; seperti apa alur kerja yang aman dan dapat diaudit; risiko teknis, etis, hukum, serta manajerial apa yang harus dikendalikan; dan bagaimana uji coba di lapas/rutan Indonesia sebaiknya dievaluasi. Tujuannya ialah menghasilkan rancangan konseptual yang relevan bagi manajemen pengamanan, bukan menyimpulkan efektivitas empiris sebelum pengujian lapangan. Model yang diajukan menempatkan petugas sebagai pengambil keputusan, membatasi pemrosesan data pada tujuan yang sah, dan menghubungkan teknologi dengan prosedur respons serta pembelajaran organisasi.

Metode

Artikel menggunakan studi kepustakaan naratif-terarah dengan pendekatan konseptual. Sumber utama meliputi Undang-Undang Nomor 22 Tahun 2022 tentang Pemasarakatan, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, informasi resmi Kementerian Imigrasi dan Pemasarakatan, pedoman Perserikatan Bangsa-Bangsa mengenai keamanan dan perlakuan manusiawi, laporan evaluasi teknologi surveilans koreksional, dokumen pengujian pengenalan wajah, serta kerangka manajemen risiko kecerdasan

buatan. Sumber dipilih karena menjelaskan kebutuhan operasional, fungsi teknologi, bukti kinerja, risiko hak asasi, atau tata kelola implementasi. Publikasi vendor tidak dijadikan dasar utama untuk menyimpulkan efektivitas.

Analisis dilakukan melalui lima tahap. Pertama, masalah pengamanan dikelompokkan menjadi deteksi anomali, verifikasi identitas, respons, pencatatan, dan pengawasan manajerial. Kedua, kemampuan serta keterbatasan analitik audio dan biometrik dipetakan terhadap masalah tersebut. Ketiga, bukti empiris dibedakan dari klaim konseptual dan rencana uji coba. Keempat, risiko dipetakan pada dimensi keselamatan, privasi, akurasi, bias, keamanan siber, kontinuitas operasi, dan beban kerja. Kelima, hasil sintesis diterjemahkan menjadi alur peringatan dini, persyaratan pengadaan, tahapan uji coba, serta indikator evaluasi.

Kajian ini tidak menggunakan data primer, tidak menguji perangkat tertentu, dan tidak membandingkan akurasi produk. Karena karakter akustik, jaringan, arsitektur, populasi, dan prosedur setiap lapas/rutan berbeda, hasilnya berupa desain kebijakan dan operasi yang masih memerlukan validasi lapangan. Pernyataan mengenai manfaat dibatasi sebagai potensi, sedangkan bukti yang menunjukkan kegagalan atau peringatan palsu digunakan untuk menyusun pengenaldian serta kriteria penghentian uji coba.

Hasil

Sintesis menghasilkan model pengamanan berlapis yang terdiri atas keamanan dinamis, analitik audio, verifikasi biometrik, pusat kendali, respons berjenjang, dan tata kelola data. Teknologi ditempatkan sebagai lapisan pendukung, bukan pengganti petugas. Keamanan dinamis tetap menjadi fondasi karena hubungan profesional, komunikasi, ob-

servasi langsung, pemahaman rutinitas, dan pertukaran informasi membantu petugas mengenali perubahan suasana yang tidak selalu dapat dibaca sensor. Analitik audio memperluas jangkauan pendengaran pada area tertentu; biometrik memperkuat verifikasi identitas; sedangkan petugas menilai konteks, memilih tindakan, dan bertanggung jawab atas keputusan.

Pemetaan kebutuhan operasional

Terdapat tiga skenario prioritas. Pertama, deteksi eskalasi di lorong blok, area komunal, ruang tunggu layanan, dan titik yang sulit dipantau terus-menerus. Kedua, verifikasi warga binaan atau pengunjung pada pergerakan yang memiliki risiko salah identifikasi, seperti pintu utama, akses blok, kunjungan, klinik, dan kegiatan di luar area hunian. Ketiga, penguatan investigasi melalui penggabungan waktu peringatan, rekaman kamera, log akses, dan catatan respons. Sistem tidak diarahkan untuk merekam seluruh percakapan atau mengidentifikasi isi pembicaraan, karena tujuan tersebut melampaui kebutuhan peringatan dini dan meningkatkan risiko privasi.

Pemetaan lokasi harus mendahului pemilihan alat. Setiap area dinilai berdasarkan jenis insiden, frekuensi pergerakan, tingkat kebisingan, titik buta, ketersediaan listrik dan jaringan, pencahayaan, kelembapan, risiko vandalisme, serta kemampuan petugas merespons. Lokasi dengan suara televisi, pengeras suara, kegiatan keagamaan, percakapan kelompok, atau gema kuat mungkin menghasilkan pola yang mirip dengan target sistem. Pintu biometrik juga menghadapi variasi cahaya, posisi wajah, masker, cedera, perubahan penampilan, dan kepadatan antrean. Tanpa survei lokasi, akurasi laboratorium tidak dapat

diterjemahkan menjadi kinerja operasional.

Alur analitik audio

Alur analitik audio dimulai ketika sensor menangkap sinyal di zona yang telah ditetapkan. Perangkat mengekstraksi fitur akustik dan menghasilkan skor anomali atau klasifikasi. Jika ambang terlampaui, pusat kendali menerima peringatan yang memuat lokasi, waktu, tingkat keyakinan, dan cuplikan konteks minimum sesuai kebijakan. Petugas tidak langsung menyimpulkan terjadi perkelahian. Operator memeriksa kamera, menghubungi petugas area, atau meminta verifikasi langsung. Hasil verifikasi diklasifikasikan sebagai insiden benar, peringatan gangguan, peringatan palsu, atau tidak dapat ditentukan. Tindakan selanjutnya mengikuti prosedur respons, sementara label verifikasi digunakan untuk evaluasi berkala.

Ambang peringatan harus dapat disesuaikan per zona dan waktu. Ambang terlalu rendah menimbulkan kelelahan alarm karena petugas menerima banyak notifikasi yang tidak relevan; ambang terlalu tinggi dapat melewatkan insiden. Karena evaluasi Peterson et al. (2024) mendokumentasikan seluruh peringatan audio sebagai gangguan atau palsu selama periode pengamatan, uji coba perlu menghitung nilai prediksi positif, bukan hanya sensitivitas yang diklaim penyedia. Sistem yang banyak berbunyi tetapi tidak membantu tindakan justru menambah beban kerja dan berpotensi mengurangi kepercayaan petugas terhadap alarm yang benar.

Alur verifikasi biometrik

Biometrik diterapkan terutama untuk verifikasi satu-banding-satu. Identitas yang dinyatakan melalui kartu, jadwal pergerakan, atau daftar kunjungan dibandingkan dengan sampel wajah atau

sidik jari saat itu. Hasil cocok mengizinkan petugas melanjutkan pemeriksaan prosedural; hasil tidak cocok memicu pemeriksaan manual, bukan otomatis menyatakan penyamaran atau pelanggaran. Untuk warga binaan, data pendaftaran harus ditautkan pada identitas yang telah diverifikasi. Untuk pengunjung, tujuan, dasar pemrosesan, jangka simpan, dan hak terkait data harus dijelaskan secara layak.

Kualitas biometrik perlu diukur dengan tingkat kecocokan salah, penolakan salah, kegagalan memperoleh sampel, dan waktu transaksi. Grother, Ngan, dan Hanaoka (2019) menunjukkan bahwa algoritma pengenalan wajah dapat memiliki perbedaan tingkat kesalahan menurut karakteristik demografis dan kualitas gambar. Temuan tersebut mengharuskan pengujian menggunakan populasi, kamera, pencahayaan, sudut, serta kondisi operasional yang representatif. Penilaian agregat saja tidak cukup; hasil perlu diperiksa menurut kelompok yang relevan agar rata-rata tinggi tidak menyembunyikan kegagalan yang tidak proporsional.

Integrasi pusat kendali dan respons

Pusat kendali menggabungkan peringatan tanpa membuka akses data secara berlebihan. Tampilan ideal memprioritaskan lokasi, waktu, tingkat urgensi, status verifikasi, petugas penanggung jawab, dan langkah respons. Peringatan kritis yang terverifikasi dapat memicu pengerahan regu, dukungan medis, penguncian terbatas, atau aktivasi rencana kontingensi. Peringatan rendah dapat ditangani melalui observasi atau komunikasi. Setiap perubahan status dicatat sehingga pimpinan dapat menilai waktu sejak alarm hingga dilihat, diverifikasi, direspons, dan ditutup. Log tersebut penting untuk pembelajaran dan

akuntabilitas, bukan untuk menghukum petugas berdasarkan satu angka tanpa konteks.

Sistem wajib memiliki mode cadangan. Ketika jaringan, listrik, sensor, kamera, atau basis data biometrik bermasalah, pintu tidak boleh menciptakan bahaya evakuasi dan operasi tidak boleh berhenti tanpa alternatif. Prosedur manual, daftar otorisasi, kunci pengaman, komunikasi radio, dan pencatatan insiden tetap tersedia. Pengguna harus mengetahui siapa yang berwenang mengalihkan mode, bagaimana pemulihan dilakukan, serta kapan transaksi selama gangguan direkonsiliasi. Kontinuitas ini mencegah ketergantungan tunggal pada teknologi.

Tata kelola dan tahapan uji coba

Tata kelola mengikuti empat fungsi kerangka manajemen risiko kecerdasan buatan: mengatur, memetakan, mengukur, dan mengelola (Tabassi, 2023). Pimpinan menetapkan tujuan penggunaan, larangan penggunaan, pemilik risiko, kewenangan akses, retensi, audit, mekanisme pengaduan, dan kriteria penghentian. Tim lintas fungsi melibatkan pengamanan, teknologi informasi, registrasi, pelayanan tahanan, kesehatan, hukum, serta perlindungan data. Kontrak pengadaan harus memberi akses pada dokumentasi kinerja, pembaruan model, log, prosedur ekspor data, penghapusan data, pengujian keamanan, dan dukungan ketika perangkat gagal.

Uji coba dilakukan dalam empat fase. Fase persiapan memetakan masalah dan menetapkan kondisi awal. Fase uji senyap menjalankan sensor tanpa memengaruhi keputusan untuk mengukur pola alarm. Fase operasional terbatas mengaktifkan respons pada satu atau dua zona dengan pengawasan intensif. Fase evaluasi membandingkan hasil

dengan kondisi awal dan kelompok atau waktu pembandingan apabila memungkinkan. Perluasan hanya dilakukan jika manfaat lebih besar daripada risiko, petugas menerima sistem, alarm dapat ditindaklanjuti, perbedaan kinerja dapat dikendalikan, dan tidak terjadi pelanggaran privasi yang material.

Indikator uji coba dibagi menjadi keluaran teknis, operasional, keselamatan, dan tata kelola. Keluaran teknis mencakup ketersediaan perangkat, latensi, kualitas sinyal, kegagalan transaksi, serta tingkat alarm. Keluaran operasional meliputi waktu verifikasi, waktu respons, pekerjaan tambahan, dan kemampuan sistem mendukung investigasi. Indikator keselamatan mencakup insiden yang ditemukan lebih awal, dampak insiden, serta kejadian yang terlewat. Tata kelola dinilai melalui kepatuhan akses, jumlah koreksi data, keluhan, insiden privasi, pemeriksaan perbedaan kinerja, dan tindak lanjut audit. Satu indikator tidak boleh berdiri sendiri; respons cepat tidak dapat disebut berhasil apabila didapat melalui alarm palsu berlebihan atau pelanggaran hak.

Hasil evaluasi perlu dibahas dalam forum peninjauan yang memiliki kewenangan memperbaiki konfigurasi dan prosedur. Forum memeriksa contoh alarm benar dan salah, kondisi yang menyebabkannya, respons petugas, serta konsekuensi bagi warga binaan. Perubahan ambang, pemindahan sensor, penambahan pencahayaan, atau penyederhanaan alur harus dicatat sebagai versi baru agar dampaknya dapat dibandingkan. Jika penyedia memperbarui algoritma, pengujian kinerja diulang karena perubahan model dapat mengubah tingkat kesalahan. Dengan demikian, pengawasan tidak berhenti pada saat serah

terima barang, tetapi berlangsung sepanjang siklus hidup sistem.

Pembahasan

Model ini mengubah gagasan awal teknologi pengamanan dari pengganti pengawasan manusia menjadi alat bantu keputusan. Perubahan tersebut penting karena kata seperti kecerdasan buatan, deteksi agresi, dan pengenalan wajah sering menimbulkan kesan kepastian. Padahal, keluaran sistem merupakan prediksi berdasarkan data, ambang, dan kondisi sensor. Suara keras dapat berasal dari konflik, kegiatan bersama, panggilan bantuan, atau gema. Ketidakcocokan wajah dapat disebabkan penyamaran, tetapi juga pencahayaan, posisi, kamera, atau perubahan penampilan. Keputusan yang sah memerlukan verifikasi manusia dan informasi kontekstual.

Analitik audio memiliki nilai potensial pada kecepatan dan cakupan. Sensor dapat aktif terus-menerus dan menandai zona yang tidak sedang menjadi fokus operator. Namun, manfaat hanya muncul ketika alarm relevan dan tersedia kapasitas respons. Bukti empiris yang ditemukan belum mendukung klaim bahwa pemasangan otomatis menurunkan kekerasan. Evaluasi di Minnesota justru menunjukkan masalah integrasi dan peringatan palsu. Oleh karena itu, indikator keberhasilan tidak boleh berupa jumlah alarm atau jumlah perangkat terpasang. Ukuran yang lebih bermakna ialah proporsi alarm terverifikasi, insiden yang ditemukan lebih awal, perubahan waktu respons, pengurangan konsekuensi insiden, dan beban tambahan pada petugas.

Biometrik juga harus diposisikan sebagai faktor verifikasi, bukan satu-satunya otoritas. Pada titik akses berisiko tinggi, verifikasi wajah atau sidik jari dapat melengkapi kartu, jadwal, pemerik-

retensi pendek, mengenkripsi data, dan mencatat setiap akses.

Transparansi tetap diperlukan meskipun lingkungan lapas/rutan memiliki kebutuhan keamanan khusus. Warga binaan, petugas, dan pengunjung perlu memperoleh informasi mengenai jenis teknologi, tujuan, area penggunaan, data yang diproses, jangka simpan, pihak yang dapat mengakses, serta saluran koreksi atau pengaduan. Transparansi tidak berarti membuka konfigurasi yang dapat dieksploitasi. Informasi operasional sensitif dapat dibatasi, tetapi keberadaan dan prinsip penggunaan sistem tidak selayaknya dirahasiakan dari pihak yang terdampak.

Keamanan siber merupakan bagian dari keamanan fisik. Basis data biometrik, kamera jaringan, sensor, dan pusat kendali dapat menjadi sasaran pencurian kredensial, manipulasi log, perangkat lunak berbahaya, atau gangguan layanan. Arsitektur perlu memisahkan jaringan, menggunakan autentikasi kuat, pembaruan terkontrol, pencadangan, inventaris aset, pemantauan akses, dan pengujian pemulihan. Akun bersama harus dihindari agar tindakan dapat ditelusuri. Penyedia tidak boleh memiliki akses jarak jauh permanen tanpa persetujuan, batas waktu, dan pencatatan.

Kesiapan SDM menentukan keberhasilan. Pelatihan tidak cukup menjelaskan tombol dan menu, tetapi harus mencakup makna skor, jenis kesalahan, cara verifikasi, batas kewenangan, perlindungan data, respons darurat, serta pelaporan gangguan. Simulasi perlu menggunakan skenario nyata: teriakan saat olahraga, kegagalan wajah pada cahaya rendah, antrean mendadak, kehilangan jaringan, dan alarm bersamaan. Petugas juga harus dilibatkan sejak pemetaan kebutuhan agar teknologi menyelesaikan

masalah yang benar dan tidak menambah pekerjaan pencatatan ganda.

Dari sisi anggaran, biaya siklus hidup lebih penting daripada harga pembelian. Perhitungan meliputi survei lokasi, kabel, jaringan, server, lisensi, penyimpanan, pemeliharaan, suku cadang, pembaruan, audit, pelatihan pegawai baru, dan penggantian perangkat. Pengadaan yang hanya mengejar spesifikasi tertinggi dapat menghasilkan sistem kompleks yang tidak terpelihara. Pilihan yang lebih rasional adalah skala kecil dengan manfaat terukur, interoperabilitas, data yang dapat diekspor, serta kemampuan lembaga menghentikan layanan tanpa kehilangan akses terhadap catatannya sendiri.

Efektivitas pilot perlu dinilai melalui desain evaluasi yang disiplin. Data kondisi awal mencakup jumlah insiden, lokasi, waktu penemuan, waktu respons, kualitas bukti, jumlah salah identifikasi, beban kerja, dan persepsi pengguna. Selama pilot dicatat sensitivitas terhadap insiden yang diketahui, nilai prediksi positif, peringatan per zona, penolakan biometrik salah, waktu transaksi, downtime, keluhan, dan insiden privasi. Analisis juga memisahkan jam sibuk, kondisi cahaya, tingkat kebisingan, serta kelompok demografis yang relevan. Tanpa kondisi awal dan definisi indikator, peningkatan tidak dapat dibedakan dari persepsi kebaruan.

Penggunaan hasil sistem dalam pemeriksaan disiplin memerlukan aturan pembuktian yang ketat. Alarm hanya menunjukkan bahwa sistem menemukan pola tertentu; ia bukan kesaksian dan bukan rekonstruksi lengkap. Rekaman, log, observasi petugas, keterangan pihak terkait, dan bukti lain harus diperiksa secara proporsional. Warga binaan perlu memperoleh kesempatan menjelaskan keadaan dan mengoreksi identitas atau data yang keliru. Pemisahan antara fungsi

peringatan, investigasi, dan penetapan konsekuensi mencegah prediksi teknis berubah menjadi hukuman otomatis serta menjaga proses yang adil.

Perubahan organisasi juga perlu dipantau. Teknologi dapat menggeser pola patroli, perhatian operator, pembagian tugas, dan hubungan petugas dengan warga binaan. Jika operator terlalu berfokus pada layar, informasi yang diperoleh melalui komunikasi langsung dapat berkurang. Sebaliknya, bila sistem mengurangi pemeriksaan identitas berulang yang tidak perlu, petugas dapat memusatkan waktu pada interaksi substantif dan deteksi risiko. Evaluasi karena itu harus menanyakan bukan hanya apakah perangkat bekerja, tetapi bagaimana perangkat mengubah pekerjaan, diskresi, komunikasi, dan budaya keamanan.

Keterbatasan kajian

Model memiliki keterbatasan. Pertama, kajian tidak menguji perangkat pada lapas/rutan Indonesia. Kedua, bukti analitik audio koreksional yang tersedia masih sedikit dan tidak dapat digeneralisasi. Ketiga, pengujian pengenalan wajah NIST menggambarkan variasi algoritma dan data, bukan kinerja satu sistem pada konteks Indonesia. Keempat, angka kepadatan nasional tidak menjelaskan kebutuhan setiap unit. Penelitian selanjutnya perlu melakukan uji lapangan multisitus, melibatkan petugas dan warga binaan, mengukur dampak terhadap keselamatan serta hak, dan membandingkan teknologi dengan perbaikan nonteknologis seperti penambahan petugas, penataan patroli, pencahayaan, dan pengurangan titik buta.

Kesimpulan

Analitik audio dan pemindai biometrik dapat mendukung peringatan dini serta verifikasi identitas di lapas/ru-

tan apabila ditempatkan dalam pengamanan berlapis. Analitik audio berfungsi memicu pemeriksaan terhadap anomali, sedangkan biometrik memperkuat verifikasi satu-banding-satu pada titik akses. Keduanya tidak membuktikan agresi atau pelanggaran secara otomatis. Petugas tetap memverifikasi konteks, menentukan respons, dan mempertanggungjawabkan keputusan.

Penerapan yang layak memerlukan pemetaan lokasi, uji senyap, pilot terbatas, prosedur cadangan, perlindungan data sejak desain, audit kinerja, keamanan siber, serta evaluasi atas alarm palsu dan perbedaan tingkat kesalahan. Bukti yang tersedia, khususnya evaluasi analitik audio di penjara Minnesota, menunjukkan bahwa teknologi dapat menghasilkan alarm gangguan tanpa mendeteksi agresi yang dimaksud. Karena itu, keputusan perluasan harus didasarkan pada manfaat terukur terhadap waktu respons, kualitas verifikasi, keselamatan, beban kerja, keadilan, dan privasi, bukan pada jumlah perangkat atau daya tarik inovasi.

Implikasi

Secara kebijakan, Direktorat Jenderal Pemasyarakatan perlu menyusun standar minimum penggunaan analitik audio dan biometrik yang menetapkan tujuan, area terlarang, dasar pemrosesan, retensi, hak akses, audit, pengaduan, pengujian bias, dan akuntabilitas keputusan. Secara manajerial, kepala lapas/rutan perlu membentuk tim lintas fungsi, menetapkan indikator kondisi awal, menunjuk pemilik risiko, serta memastikan kontrak pengadaan tidak mengunci data dan pemeliharaan pada penyedia tunggal.

Secara praktis, pilot sebaiknya dimulai pada satu zona dan satu titik akses dengan risiko yang jelas. Uji senyap di-

lakukan sebelum alarm memengaruhi tindakan. Hasil ditinjau secara berkala bersama petugas operasional, teknologi informasi, hukum, dan perlindungan data. Sistem dihentikan atau dirancang ulang apabila alarm palsu berlebihan, manfaat tidak terukur, terjadi perbedaan kinerja yang tidak dapat dikendalikan, operasi terganggu, atau risiko privasi melampaui manfaat. Penelitian lanjutan perlu membandingkan biaya dan hasil teknologi dengan intervensi organisasi agar inovasi benar-benar memperkuat keamanan yang manusiawi.

Referensi

- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT), Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
- Kementerian Imigrasi dan Pemasyarakatan Republik Indonesia. (2026, April 10). Overcrowding lapas menurun, Menteri Imipras pertegas komitmen berantas narkoba. <https://kemenimipras.go.id/berita-utama/overcrowding-lapas-menurun-menteri-imipras-pertegas-komitmen-berantas-narkoba>
- Peterson, B. E., Shukla, R., Lawrence, D. S., & Robin, L. (2024). Optimizing video surveillance in correctional settings (NCJ 308634). Urban Institute. <https://www.ojp.gov/pdf-files1/nij/grants/308634.pdf>
- Republik Indonesia. (2022a). Undang-Undang Republik Indonesia Nomor 22 Tahun 2022 tentang Pemasyarakatan.
- Republik Indonesia. (2022b). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Singapore Prison Service. (2025, April 15).

SPS-YRSG Corporate Advance 2025:

Forward corrections—innovate and collaborate.

<https://www.sps.gov.sg/sps-yrsg-corporate-advance-2025/>

Tabassi, E. (2023). Artificial Intelligence

Risk Management Framework (AI

RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology.

<https://doi.org/10.6028/NIST.AI.100-1>

United Nations Office on Drugs and

Crime. (2015). Handbook on dynamic security and prison intelligence.

United Nations.

United Nations Office on Drugs and

Crime. (2015). The United Nations

Standard Minimum Rules for the

Treatment of Prisoners (the Nelson Mandela Rules). United Nations.