

PEMANFAATAN INTERNET OF THINGS (IoT) UNTUK KEAMANAN DAN KONTROL AKTIVITAS NARAPIDANA DI LEMBAGA PEMASYARAKATAN

Gigih Nanda Wirayuda

Program Studi Manajemen Pemasyarakatan, Politeknik Imigrasi dan Pemasyarakatan Indonesia

Journal of Correctional Management
2026, Vol.3 (1) 31 - 10
Politeknik Ilmu Pemasyarakatan

Review
24-05-2026

Accepted
25-06-2026

DOI. <https://doi.org/10.52472/jcm.v3i1.790>

Abstract

Indonesian correctional institutions need security systems that can respond to overcrowding, limited personnel, prohibited-goods trafficking, violence, and escape risk without reducing prisoners to permanent objects of surveillance. This article examines the lawful use of the Internet of Things (IoT) for prison security and the control of prisoner activities. It applies normative legal research through statutory, conceptual, and comparative approaches to correctional law, personal data protection, electronic-system governance, cybersecurity standards, and international prisoner-treatment principles. The study finds that intelligent cameras, biometric access controls, wearable devices, and environmental sensors may strengthen early warning, accountability, and emergency response. Nevertheless, biometric, location, health, and behavioral data create high risks of excessive surveillance, cyber incidents, algorithmic discrimination, and unclear liability. Indonesia therefore requires a risk-based regulatory model founded on legality, necessity, proportionality, data minimization, human oversight, security by design, independent audit, and effective remedies. IoT should support professional correctional judgment, not replace it.

Keywords: *Internet of Things; correctional institution; security; personal data; prisoners' rights*

Abstrak

Lembaga pemasyarakatan di Indonesia memerlukan sistem keamanan yang mampu menjawab kepadatan hunian, keterbatasan petugas, peredaran barang terlarang, kekerasan, dan risiko pelarian tanpa menjadikan narapidana sebagai objek pengawasan tanpa batas. Artikel ini mengkaji penggunaan Internet of Things (IoT) yang sah untuk keamanan dan kontrol aktivitas narapidana. Penelitian hukum normatif dilakukan melalui pendekatan perundang-undangan, konseptual, dan perbandingan terhadap hukum pemasyarakatan, perlindungan data pribadi, tata kelola sistem elektronik, keamanan siber, dan prinsip internasional perlakuan terhadap narapidana. Hasil kajian menunjukkan bahwa kamera cerdas, kontrol akses biometrik, perangkat yang dapat dikenakan, dan sensor lingkungan dapat memperkuat peringatan dini, akuntabilitas, serta respons kedaruratan. Namun, pemrosesan data biometrik, lokasi, kesehatan, dan perilaku menimbulkan risiko pengawasan berlebihan, insiden siber, diskriminasi algoritmik, dan ketidakjelasan pertanggungjawaban. Karena itu, Indonesia memerlukan model regulasi berbasis risiko yang bertumpu pada legalitas, kebutuhan, proporsionalitas, minimisasi data, kendali manusia, keamanan sejak perancangan, audit independen, dan pemulihan yang efektif. IoT harus mendukung, bukan menggantikan, penilaian profesional petugas pemasyarakatan.

Kata kunci: *Internet of Things; pemasyarakatan; keamanan; data pribadi; hak narapidana*

Pendahuluan

Perkembangan teknologi digital mengubah cara negara mengelola pelayanan publik, termasuk penyelenggaraan fungsi pemasyarakatan. Internet of Things (IoT) memungkinkan sensor, kamera, pengendali akses, perangkat komputasi, dan aplikasi terhubung untuk mengumpulkan serta menukar data secara otomatis. International Telecommunication Union (2012) menempatkan IoT sebagai infrastruktur masyarakat informasi yang menghubungkan objek fisik dan virtual melalui teknologi informasi dan komunikasi yang interoperabel. Dalam lembaga pemasyarakatan (Lapas), kemampuan tersebut dapat digunakan untuk mendeteksi pergerakan pada area steril, mengendalikan pintu, mengenali kondisi darurat, mencatat akses, dan mengirimkan peringatan kepada petugas secara waktu nyata.

Kebutuhan modernisasi muncul karena pengamanan Lapas berlangsung dalam lingkungan yang kompleks. Kepadatan hunian, keterbatasan rasio petugas terhadap penghuni, keragaman tingkat risiko, peredaran barang terlarang, kekerasan, gangguan kesehatan, kebakaran, dan upaya pelarian menuntut pengawasan yang konsisten. Sistem konvensional yang hanya mengandalkan patroli dan pemantauan layar memiliki keterbatasan perhatian, jangkauan, dan kesinambungan. IoT dapat memperluas kemampuan deteksi dan menyediakan jejak audit, tetapi teknologi ini tidak boleh diposisikan sebagai pengganti petugas. Informasi dari sensor tetap memerlukan verifikasi, konteks, diskresi, serta keputusan manusia yang bertanggung jawab.

Penerapan IoT di Lapas juga berbeda dari penggunaannya pada ruang publik biasa. Narapidana berada dalam hubungan kuasa yang tidak seimbang

dengan negara dan tidak bebas menghindari kamera, sensor biometrik, atau pelacak lokasi. Data yang dihasilkan dapat mengungkapkan identitas, catatan kejahatan, kesehatan, kebiasaan, relasi sosial, lokasi, bahkan prediksi perilaku. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menggolongkan data biometrik, data kesehatan, dan catatan kejahatan sebagai data pribadi spesifik. Konsekuensinya, peningkatan keamanan tidak dapat dijadikan alasan umum untuk mengumpulkan semua data, memantau seluruh ruang, atau menyimpan rekaman tanpa batas waktu.

Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan memberi dasar bagi pelaksanaan fungsi pengamanan dan pengamatan, tetapi pada saat yang sama mewajibkan penghormatan, pelindungan, dan pemenuhan hak asasi manusia. Orientasi ini sejalan dengan Pasal 10 International Covenant on Civil and Political Rights yang menegaskan perlakuan manusiawi dan penghormatan terhadap martabat setiap orang yang dirampas kebebasannya (Office of the United Nations High Commissioner for Human Rights, 1966). Nelson Mandela Rules juga menempatkan martabat, keselamatan, layanan kesehatan, dokumentasi, dan akuntabilitas sebagai standar dasar pengelolaan penjara (United Nations, 2015). Dengan demikian, keamanan dan hak narapidana bukan dua tujuan yang saling meniadakan, melainkan kewajiban yang harus dirancang secara bersamaan.

Masalah utama terletak pada belum adanya pengaturan khusus yang menghubungkan fungsi pengamanan Lapas dengan siklus hidup data IoT. Kerangka yang tersedia tersebar dalam UU Pemasyarakatan, UU PDP, rezim Informasi dan Transaksi Elektronik yang

terakhir diubah melalui Undang-Undang Nomor 1 Tahun 2024, Peraturan Pemerintah Nomor 71 Tahun 2019, pedoman keamanan SPBE, perlindungan infrastruktur informasi vital, dan Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 mengenai penyelenggara sistem elektronik lingkup publik. Fragmentasi ini menyisakan pertanyaan tentang dasar pemrosesan, batas ruang pengawasan, masa retensi, akses vendor, penggunaan analitik otomatis, pertanggungjawaban ketika sistem gagal, serta mekanisme pengaduan narapidana.

Berangkat dari persoalan tersebut, penelitian ini menjawab tiga pertanyaan. Pertama, bentuk pemanfaatan IoT apa yang relevan bagi keamanan dan kontrol aktivitas narapidana? Kedua, bagaimana kerangka hukum Indonesia menilai pemrosesan data dan risiko yang ditimbulkannya? Ketiga, model tata kelola apa yang dapat menyeimbangkan efektivitas pengamanan dengan hak asasi manusia? Kebaruan kajian terletak pada penyusunan model regulasi berbasis risiko yang menggabungkan hukum masyarakatan, perlindungan data, keamanan sistem elektronik, pengawasan algoritmik, dan akuntabilitas vendor ke dalam satu kerangka implementasi.

Metode

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan. Pendekatan perundang-undangan digunakan untuk menelaah hubungan antara mandat pengamanan dalam UU Masyarakatan, prinsip dan kewajiban pemrosesan dalam UU PDP, keandalan sistem elektronik dalam PP Nomor 71 Tahun 2019, perubahan kedua UU ITE, standar keamanan SPBE, dan tata kelola sistem elektronik lingkup publik. Pen-

dekatan konseptual digunakan untuk menguji legalitas, kebutuhan, proporsionalitas, minimisasi data, privacy by design, security by design, kendali manusia, dan akuntabilitas. Pendekatan perbandingan memakai Directive (EU) 2016/680 sebagai pembanding karena instrumen tersebut secara khusus mengatur data pribadi untuk penegakan hukum dan pelaksanaan pidana.

Bahan hukum primer meliputi peraturan perundang-undangan Indonesia, ICCPR, Nelson Mandela Rules, dan Directive (EU) 2016/680. Bahan sekunder mencakup literatur penelitian hukum, standar teknis IoT, kerangka keamanan siber, serta laporan evaluasi pengenalan wajah. Sumber dipilih berdasarkan relevansi terhadap lingkungan masyarakatan, otoritas penerbit, status berlaku, dan keterkaitan dengan pemrosesan berisiko tinggi. Analisis dilakukan melalui inventarisasi norma, identifikasi konflik dan kekosongan pengaturan, penafsiran sistematis, serta penyusunan rekomendasi preskriptif sebagaimana karakter penelitian hukum normatif (Soekanto & Mamudji, 2003; Marzuki, 2017). Kajian ini tidak mengukur efektivitas perangkat di Lapas tertentu sehingga istilah manfaat digunakan sebagai potensi normatif-teknis, bukan sebagai klaim kausal atau statistik.

Hasil

Arsitektur dan fungsi IoT di Lapas

Hasil pemetaan menunjukkan empat kelompok teknologi yang paling relevan. Pertama, kamera cerdas dan video analytics dapat mendeteksi pergerakan pada zona terlarang, kerumunan, perkelahian, benda yang ditinggalkan, atau pola lain yang telah ditentukan. Kedua, kontrol akses biometrik dan radio-frequency identification dapat memverifikasi petugas atau penghuni, mencatat

waktu serta lokasi akses, dan mendukung penguncian terpusat. Ketiga, wearable devices dapat memantau lokasi dalam area tertentu atau mendukung program pembimbingan di luar Lapas. Keempat, sensor lingkungan dapat mendeteksi asap, suhu, gas, getaran, kebisingan abnormal, kerusakan pagar, serta kondisi teknis lain yang memerlukan respons cepat.

Keempat kelompok tersebut membentuk rantai pemrosesan yang sama: perangkat mengumpulkan data, jaringan mengirimkannya, platform menyimpan atau menganalisisnya, antarmuka menampilkan peringatan, dan petugas mengambil tindakan. Manfaat keamanan hanya muncul apabila seluruh rantai berfungsi. Sensor yang akurat tetapi jaringan terputus tidak menghasilkan peringatan; analitik yang cepat tetapi tidak memiliki prosedur verifikasi dapat menghasilkan tindakan keliru; sedangkan sistem kunci elektronik tanpa mekanisme manual dapat memperbesar bahaya saat kebakaran atau kegagalan listrik. Karena itu, redundansi, mode luring, sumber daya cadangan, prosedur fail-safe, dan latihan kedaruratan merupakan bagian dari desain hukum-operasional, bukan sekadar spesifikasi teknis.

Interoperabilitas perlu dibatasi secara sadar. Integrasi antara sistem keamanan, registrasi, kesehatan, pembinaan, dan pembimbingan memang dapat mengurangi duplikasi, tetapi sekaligus memperbesar profil digital setiap narapidana. Tidak semua data yang tersedia harus dapat diakses melalui satu dasbor. Pertukaran data seharusnya menggunakan pengenalan, atribut, dan antarmuka minimum yang diperlukan untuk satu tujuan yang telah ditetapkan. Kualitas data juga menjadi syarat penting karena identitas ganda, waktu perangkat yang tidak sinkron, sensor yang tidak terkalibrasi,

atau lokasi yang keliru dapat menghasilkan rangkaian keputusan yang salah. Karena itu, tata kelola IoT perlu menetapkan sumber data otoritatif, validasi sebelum integrasi, pencatatan perubahan, mekanisme koreksi, dan pemisahan antara data faktual dengan skor atau prediksi. Prinsip ini mencegah perluasan fungsi secara diam-diam dan menjaga agar informasi keamanan tidak berubah menjadi profil perilaku permanen.

Peta kewajiban hukum

UU Pemasyarakatan menjadi dasar tujuan penggunaan: teknologi harus mendukung pelayanan, pembinaan, perawatan, pengamanan, dan pengamatan yang menghormati hak asasi manusia. UU PDP mengatur jenis data, dasar pemrosesan, hak subjek data, kewajiban pengendali dan prosesor, keamanan, rekam jejak kegiatan, penilaian dampak, serta pemberitahuan kegagalan perlindungan data. Untuk Lapas, persetujuan narapidana pada umumnya bukan dasar yang ideal karena ketimpangan kekuasaan dapat mengurangi kebebasan persetujuan. Pemrosesan seharusnya ditautkan pada kewajiban hukum atau pelaksanaan tugas untuk kepentingan umum, kemudian dibatasi oleh tujuan yang spesifik dan ukuran proporsionalitas.

Rezim sistem elektronik melengkapi kewajiban tersebut. PP Nomor 71 Tahun 2019 menuntut penyelenggaraan sistem yang andal, aman, dan bertanggung jawab; Peraturan BSSN Nomor 4 Tahun 2021 memberi pedoman manajemen keamanan informasi dan prosedur keamanan SPBE; Peraturan BSSN Nomor 8 Tahun 2024 mengatur audit keamanan SPBE; sedangkan Permenkomdigi Nomor 5 Tahun 2025 memperbarui tata kelola penyelenggara sistem elektronik lingkup publik, termasuk klasifikasi data berdasarkan risiko. Apabila sis-

tem IoT Lapas diidentifikasi sebagai bagian dari infrastruktur informasi vital sektor administrasi pemerintahan, Peraturan Presiden Nomor 82 Tahun 2022 dan aturan turunannya menambah kebutuhan identifikasi, perlindungan, pembinaan, pengawasan, serta koordinasi insiden.

Empat rumpun risiko utama

Pertama, risiko hak dan privasi muncul dari pemantauan berkelanjutan, pengumpulan data yang melampaui tujuan, penggunaan rekaman untuk kepentingan lain, serta hilangnya ruang privat minimum. Kamera pada area kunjungan, layanan kesehatan, kamar mandi, atau ruang ibadah memerlukan pembatasan yang jauh lebih ketat dibanding kamera pada perimeter dan jalur akses. Kedua, risiko keamanan siber mencakup pengambilalihan akun, manipulasi sensor, pembukaan kunci tanpa hak, ransomware, kebocoran data biometrik, dan gangguan layanan. Data biometrik tidak dapat diganti seperti kata sandi sehingga akibat kebocorannya bersifat jangka panjang.

Ketiga, analitik otomatis dapat menghasilkan salah deteksi dan diskriminasi. Evaluasi NIST menemukan adanya perbedaan kinerja demografis pada banyak algoritma pengenalan wajah yang diuji, walaupun besarnya berbeda antaralgoritma dan kualitas citra berpengaruh terhadap hasil (Grother et al., 2019). Dalam Lapas, false positive dapat menyebabkan pemeriksaan, pembatasan, atau pelabelan risiko yang tidak semestinya. Keempat, terdapat risiko ketidakjelasan tanggung jawab antara unit pelaksana teknis, kementerian, pengelola pusat data, integrator, vendor perangkat, penyedia komputasi awan, dan petugas yang merespons alarm. Kontrak pengadaan tidak boleh mengalihkan kewa-

jiban publik atau menghilangkan tanggung jawab pengendali data.

Arah pembelajaran komparatif

Directive (EU) 2016/680 menunjukkan pentingnya aturan khusus untuk data yang diproses oleh otoritas berwenang dalam pencegahan, penyelidikan, penuntutan, dan pelaksanaan pidana. Instrumen tersebut menekankan tujuan yang ditentukan, akurasi, batas penyimpanan, keamanan, hak subjek data, pencatatan kegiatan, penilaian dampak, petugas perlindungan data, serta pengawasan independen. Pelajaran yang dapat diadopsi bukan menyalin rezim Eropa, melainkan membedakan tata kelola data masyarakatan dari pemrosesan administratif biasa. Posisi narapidana yang rentan dan potensi konsekuensi fisik dari keputusan sistem membenarkan perlindungan yang lebih spesifik.

Pembahasan

Legalitas, kebutuhan, dan proporsionalitas

Model yang ideal dimulai dari definisi tujuan pada setiap perangkat. Kamera perimeter dapat ditujukan untuk mencegah pelarian; sensor asap untuk keselamatan; kontrol biometrik untuk mencegah akses tanpa hak; dan wearable device untuk pengawasan berdasarkan penilaian risiko. Tujuan yang luas seperti 'demi keamanan' tidak memadai karena tidak membatasi jenis data, ruang, subjek, penerima, atau masa simpan. Setiap penerapan harus menjawab apakah teknologi tersebut memiliki dasar kewenangan, benar-benar diperlukan, mampu mencapai tujuan, dan tidak tersedia cara lain yang lebih ringan tetapi sama efektifnya.

Uji proporsionalitas perlu dilakukan pada tiga tingkat. Kesesuaian menilai hubungan rasional antara fitur

dan risiko. Kebutuhan membandingkan pilihan teknologi dengan patroli, desain bangunan, penambahan pencahayaan, penguatan prosedur, atau penempatan petugas. Keseimbangan menilai apakah manfaat keamanan sebanding dengan pembatasan hak dan kemungkinan salah. Pemantauan biometrik berkelanjutan seluruh penghuni tidak otomatis sah hanya karena secara teknis tersedia. Intensitas pengawasan harus bertingkat berdasarkan lokasi, waktu, jenis insiden, dan asesmen risiko individual yang dapat ditinjau kembali. Area privat minimum harus dilindungi; pengecualian hanya dapat dilakukan untuk risiko keselamatan yang nyata, terbatas waktu, terdokumentasi, dan diawasi.

Pelindungan data dan keamanan sejak perancangan

Karena IoT Lapas memproses data spesifik, melakukan pemantauan sistematis, dan dapat memakai teknologi baru serta keputusan otomatis, penilaian dampak pelindungan data harus dilakukan sebelum pengadaan atau uji coba. Penilaian tersebut sekurang-kurangnya memetakan aliran data, dasar hukum, tujuan, kategori subjek, titik pengumpulan, integrasi antarsistem, penerima, lokasi penyimpanan, retensi, akses vendor, risiko terhadap hak, mitigasi, dan risiko residual. Hasilnya menjadi dasar keputusan apakah proyek dilanjutkan, diubah, dibatasi, atau dihentikan. Penilaian harus diperbarui ketika tujuan, algoritma, vendor, jenis sensor, atau skala pemrosesan berubah.

Minimisasi data dapat diterapkan dengan mengurangi resolusi atau bidang pandang pada area tertentu, melakukan pemrosesan di perangkat, menggunakan deteksi peristiwa tanpa identifikasi wajah apabila identitas tidak diperlukan, memisahkan basis data keamanan dari data pembinaan, serta menghapus data

secara otomatis setelah masa retensi berakhir. Akses harus berbasis peran dan prinsip least privilege, diperkuat autentikasi multifaktor, enkripsi saat tersimpan dan dikirim, pencatatan yang tidak mudah diubah, pengujian kerentanan, pembaruan perangkat lunak, inventaris perangkat, segmentasi jaringan, pencadangan, dan rencana pemulihan. Prinsip ini sejalan dengan panduan keamanan perangkat IoT NIST (Fagan et al., 2021) serta fungsi govern, identify, protect, detect, respond, dan recover dalam NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology, 2024).

Penggunaan pengenalan wajah atau analitik perilaku memerlukan perlindungan tambahan. Sebelum digunakan, algoritma harus diuji pada kondisi pencahayaan, sudut kamera, kepadatan, dan demografi yang menyerupai lingkungan sasaran. Ambang keputusan, tingkat false positive dan false negative, serta keterbatasan model harus didokumentasikan. Alarm tidak boleh langsung menjadi dasar hukuman disiplin, perubahan klasifikasi risiko, atau pembatasan hak. Petugas wajib memeriksa bukti lain, memberi alasan, dan menyediakan jalur koreksi. Pengadaan juga harus melarang vendor memakai rekaman untuk melatih model lain tanpa dasar hukum dan persetujuan kelembagaan yang sah.

Akuntabilitas kelembagaan dan vendor

Kementerian dan unit pelaksana teknis harus menetapkan secara tertulis siapa pengendali data, siapa prosesor, siapa pemilik sistem, dan siapa penanggung jawab operasional. Pengendali tetap bertanggung jawab menentukan tujuan dan sarana pemrosesan meskipun perangkat, platform, atau pusat data dikelola vendor. Kontrak harus mengatur standar keamanan, lokasi data, subprosesor, kerahasiaan personel, hak audit,

pengembalian dan penghapusan data, dukungan pembaruan, pelaporan insiden, keberlanjutan layanan, kepemilikan log, larangan penguncian vendor, serta ganti rugi tanpa mengurangi tanggung jawab publik kepada narapidana.

Setiap Lapas perlu memiliki prosedur respons berjenjang. Alarm teknis harus diklasifikasikan, diverifikasi, dicatat, dan dievaluasi. Insiden keselamatan memerlukan jalur prioritas berbeda dari anomali perangkat. Kegagalan perlindungan data harus ditangani melalui isolasi, preservasi bukti, analisis dampak, pemulihan, dan pemberitahuan sesuai UU PDP. Kegagalan kunci elektronik harus memicu mekanisme manual yang aman. Audit berkala perlu menilai bukan hanya kepatuhan dokumen, tetapi juga log akses, akurasi alarm, penundaan respons, ketepatan retensi, status pembaruan perangkat, pemenuhan kontrak, keluhan penghuni, dan dampak berbeda terhadap kelompok tertentu. Temuan audit harus menghasilkan koreksi yang dapat ditelusuri.

Model regulasi berbasis risiko

Regulasi teknis masyarakatan perlu membagi teknologi ke dalam tiga tingkat. Risiko rendah meliputi sensor keselamatan nonidentifikasi pada perimeter atau fasilitas. Risiko menengah mencakup CCTV area umum, pencatatan akses, dan sensor yang dapat dikaitkan dengan identitas. Risiko tinggi meliputi biometrik, pelacakan individu secara berkelanjutan, pemantauan kesehatan, pengenalan wajah, analitik perilaku, dan keputusan otomatis. Semakin tinggi tingkat risiko, semakin ketat syarat dasar hukum, penilaian dampak, uji independen, persetujuan berjenjang, retensi, audit, transparansi, dan kendali manusia. Klasifikasi harus memperhitungkan kombinasi sistem karena data yang tampak tidak

sensitif dapat menjadi sangat invasif setelah digabungkan.

Implementasi sebaiknya dimulai melalui pilot project dengan kriteria keberhasilan yang terukur, antara lain penurunan waktu respons, akurasi deteksi, ketersediaan sistem, jumlah alarm palsu, keselamatan penghuni, kepatuhan retensi, insiden keamanan siber, dan penerimaan petugas. Pilot tidak boleh hanya menilai apakah perangkat berfungsi, tetapi juga apakah tujuan dapat dicapai tanpa dampak hak yang tidak proporsional. Evaluasi harus melibatkan unsur pengamanan, pembinaan, teknologi informasi, hukum, perlindungan data, kesehatan, pengawasan internal, dan representasi kepentingan penghuni. Sistem baru dapat diperluas setelah risiko residual diterima secara tertulis dan rencana koreksi tersedia.

Transparansi tidak berarti membuka detail yang dapat melemahkan keamanan. Narapidana tetap perlu memperoleh informasi yang mudah dipahami mengenai kategori data, tujuan, dasar hukum, masa simpan, pihak yang dapat mengakses, penggunaan keputusan otomatis, serta cara mengajukan keberatan atau koreksi. Rambu pada area pengawasan, pemberitahuan tertulis saat admisi, dan penjelasan khusus untuk wearable device merupakan bentuk minimum. Jalur pengaduan harus aman dari pembalasan, dicatat, ditangani dalam batas waktu, dan dapat dieskalasikan kepada pengawas yang independen. Mekanisme ini memperkuat legitimasi sekaligus membantu mendeteksi praktik yang tidak terlihat melalui audit teknis.

Pada akhirnya, teknologi yang aman memerlukan organisasi yang siap. Petugas harus dilatih mengenali keterbatasan sistem, menjaga kerahasiaan, memverifikasi alarm, menggunakan diskresi, dan merespons insiden. Beban

kerja baru seperti pemantauan notifikasi, pemeliharaan perangkat, evaluasi log, serta pemenuhan hak subjek data harus dihitung dalam desain organisasi. IoT yang dipasang tanpa pemilik proses, anggaran pemeliharaan, dukungan suku cadang, dan pembaruan keamanan justru menciptakan rasa aman semu. Modernisasi harus dipahami sebagai perubahan tata kelola, bukan sekadar pembelian perangkat.

Kesimpulan

IoT berpotensi memperkuat pengamanan Lapas melalui kamera cerdas, kontrol akses biometrik, wearable device, dan sensor lingkungan yang terhubung dengan pusat kendali. Potensi tersebut terletak pada peringatan dini, jejak audit, pengendalian akses, keselamatan, dan respons kedaruratan. Namun, manfaat tidak bersifat otomatis dan tidak dapat dinilai hanya dari jumlah perangkat. Efektivitas bergantung pada keandalan seluruh rantai pemrosesan, verifikasi manusia, prosedur fail-safe, kapasitas petugas, serta pemeliharaan berkelanjutan.

Kerangka hukum Indonesia telah menyediakan unsur penting melalui UU Pemasarakatan, UU PDP, rezim sistem elektronik, standar keamanan SPBE, dan perlindungan infrastruktur informasi vital, tetapi pengaturannya belum terintegrasi secara khusus untuk lingkungan Lapas. Kekosongan utama mencakup klasifikasi teknologi, batas ruang pengawasan, dasar dan tujuan pemrosesan, retensi, analitik otomatis, akses vendor, kendali manusia, audit, pertanggungjawaban kegagalan, dan pemulihan bagi narapidana. Model regulasi berbasis risiko yang menerapkan legalitas, kebutuhan, proporsionalitas, minimisasi data, keamanan sejak perancangan, akuntabilitas, transparansi, dan pengawasan indepen-

den merupakan pilihan yang paling sesuai. IoT harus memperkuat profesionalitas petugas dan martabat narapidana secara bersamaan.

Implikasi

Secara normatif, Kementerian Imigrasi dan Pemasarakatan perlu menyusun regulasi teknis khusus mengenai pemanfaatan teknologi pengawasan dan pemrosesan data di Lapas. Regulasi tersebut perlu menetapkan klasifikasi risiko, daftar penggunaan yang dilarang atau dibatasi, prosedur penilaian dampak, standar retensi, persyaratan algoritma, tata kelola vendor, audit, respons insiden, transparansi, serta pengaduan. Secara kelembagaan, proyek IoT harus melalui tim lintas fungsi dan dikaitkan dengan tata kelola SPBE serta perlindungan data pribadi, bukan berdiri sebagai proyek pengadaan pengamanan semata.

Secara operasional, penerapan nasional sebaiknya didahului pilot project terbatas dan evaluasi independen. Indikator keberhasilan harus memadukan keamanan, keandalan, biaya siklus hidup, akurasi, beban kerja, keselamatan, perlindungan data, dan dampak hak asasi manusia. Penelitian lanjutan perlu menguji perangkat dalam kondisi nyata Lapas Indonesia, membandingkan hasil antar tingkat risiko, menilai pengalaman narapidana dan petugas, serta menghitung manfaat dan biaya secara transparan. Dengan pendekatan tersebut, transformasi digital pemasarakatan dapat berkembang sebagai sistem yang efektif, sah, aman, dan berorientasi pada reintegrasi sosial.

Referensi

Badan Siber dan Sandi Negara. (2021). Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sis-

- tem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik. <https://peraturan.bpk.go.id/Details/174275/peraturan-bssn-no-4-tahun-2021>
- Badan Siber dan Sandi Negara. (2024). Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik. <https://peraturan.bpk.go.id/Details/309821/peraturan-bssn-no-8-tahun-2024>
- European Parliament & Council of the European Union. (2016). Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities. Official Journal of the European Union, L 119, 89-131. <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>
- Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2021). IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (NIST SP 800-213). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-213>
- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
- Indonesia. (1999). Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. <https://peraturan.bpk.go.id/Details/45361/>
- Indonesia. (2005). Undang-Undang Republik Indonesia Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights. <https://peraturan.bpk.go.id/Details/40261/uu-no-12-tahun-2005>
- Indonesia. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. <https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019>
- Indonesia. (2022a). Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. <https://peraturan.bpk.go.id/Details/211029/perpres-no-82-tahun-2022>
- Indonesia. (2022b). Undang-Undang Republik Indonesia Nomor 22 Tahun 2022 tentang Pemasarakatan. <https://peraturan.bpk.go.id/Details/218804/uu-no-22-tahun-2022>
- Indonesia. (2022c). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. <https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024>
- International Telecommunication Union. (2012). Overview of the Internet of things (Recommendation ITU-T Y.2060). <https://www.itu.int/rec/t-rec-y.2060-201206-i>
- Kementerian Komunikasi dan Digital Republik Indonesia. (2025). Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik. <https://peraturan.bpk.go.id/Details/317335>
- Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Kencana.
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. <https://doi.org/10.6028/NIST.CSWP.29>

- Office of the United Nations High Commissioner for Human Rights. (1966). International Covenant on Civil and Political Rights. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Soekanto, S., & Mamudji, S. (2003). Penelitian hukum normatif: Suatu tinjauan singkat. RajaGrafindo Persada.
- United Nations. (2015). United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) (A/RES/70/175). <https://www.unodc.org/unodc/en/justice-and-prison-reform/nelsonmandelarules.html>