KEBEBASAN SIPIL, KEAMANAN, DAN RUANG KRITIK

Di Era Pemerintahan Digital



Keamanan demokratis melindungi warga sekaligus menjaga ruang kritik.

HAK YANG PERLU DIJAGA

- Privasi
- Kebebasan berekspresi
- Akses informasi
- Berkumpul secara damai

UJI PEMBATASAN HAK

1. Legalitas
2. Tujuan yang sah
3. Kebutuhan
4. Proporsionalitas

RISIKO DIGITAL

- Pengumpulan data berlebihan
- Kesalahan klasifikasi algoritma
- Moderasi tanpa alasan dan banding
- Efek gentar terhadap kritik

TATA KELOLA YANG AKUNTABEL

- Minimisasi data
- Audit independen
- Transparansi tujuan dan penggunaan
- Keberatan, koreksi, dan pemulihan
- Batas waktu dan evaluasi berkala

Landasan Indonesia: UUD 1945 • UU PDP 27/2022 • UU ITE 1/2024

Oleh: Prof Ir Rudy C Tarumingkeng, PhD
www.rudyct.com/cv.pdf
Guru Besar Manajemen dan AI Data Analyst, IBM-ASMI
RudyCT Academic Series

Kebebasan Sipil, Keamanan, dan Ruang Kritik di Era Pemerintahan Digital

Prof Ir Rudy C Tarumingkeng, PhD

IBM-ASMI **|** ***RudyCT Academic Series*** **|** ***www.rudyct.com/cv.pdf***

Abstract

Pemerintahan digital memperluas kapasitas negara untuk menyediakan layanan dan merespons ancaman, tetapi juga meningkatkan pengumpulan, penggabungan, serta analisis data yang dapat memengaruhi privasi, kebebasan berekspresi, dan ruang kritik. Artikel ini menjelaskan hubungan kebebasan sipil dan keamanan melalui kerangka legalitas, tujuan yang sah, kebutuhan, proporsionalitas, transparansi, pengawasan, dan pemulihan. Dalam konteks Indonesia, pembahasan mengaitkan prinsip tersebut dengan jaminan UUD 1945, Kovenan Internasional tentang Hak-Hak Sipil dan Politik, UU Pelindungan Data Pribadi, serta perubahan UU ITE tahun 2024. Argumen utamanya ialah bahwa keamanan demokratis mensyaratkan kekuasaan digital yang dapat dijelaskan dan diuji. Sistem yang efektif perlu memiliki tujuan terbatas, minimisasi data, audit independen, proses keberatan, perlindungan bagi kritik kepentingan publik, dan evaluasi berbasis bukti. Dengan tata kelola demikian, teknologi dapat meningkatkan kapasitas negara tanpa menjadikan pengawasan dan pembatasan ekspresi sebagai praktik rutin.

Kata Kunci: kebebasan sipil; keamanan publik; pemerintahan digital; kebebasan berekspresi; privasi; pengawasan algoritmik; akuntabilitas

Pendahuluan: pemerintahan digital dan batas kekuasaan

Pemerintahan digital mengubah cara negara mengenali warga, menyampaikan layanan, mengelola risiko, dan mengambil keputusan. Identitas digital, basis data terpadu, aplikasi layanan publik, kamera pengawas, analitik prediktif, serta kecerdasan buatan menjanjikan pelayanan yang lebih cepat dan kebijakan yang lebih tepat. Namun, perubahan itu juga memperluas kemampuan negara untuk mengumpulkan, menghubungkan, menyimpan, dan menafsirkan jejak kehidupan masyarakat. Pertanyaan pokoknya bukan apakah teknologi boleh digunakan, melainkan bagaimana penggunaannya dibatasi oleh hak, hukum, dan pengawasan demokratis.

Artikel ini berangkat dari tesis bahwa keamanan dan kebebasan sipil tidak harus diperlakukan sebagai dua tujuan yang saling meniadakan. Keamanan yang melindungi penduduk dari kekerasan, penipuan, serangan siber, dan bencana merupakan prasyarat bagi kehidupan bebas. Sebaliknya, kebebasan berpendapat, privasi, berkumpul, memperoleh informasi, dan mengkritik pemerintah adalah sumber koreksi yang membantu negara mengenali kesalahan serta membangun legitimasi. Ketika keselamatan dijadikan alasan terbuka tanpa batas, tindakan darurat dapat berubah menjadi kebiasaan pengawasan. Ketika hak dipahami tanpa memperhitungkan ancaman nyata, negara dapat gagal melindungi warga. Jalan yang layak ialah tata kelola berbasis hukum, bukti, pembatasan, transparansi, dan pemulihan hak.

Makna kebebasan sipil dalam negara demokratis

Kebebasan sipil adalah seperangkat hak yang melindungi ruang otonomi individu dan masyarakat dari campur tangan negara maupun aktor lain. Hak tersebut mencakup kebebasan hati nurani dan beragama, menyatakan pendapat, mencari dan menerima informasi, berserikat, berkumpul secara damai, bergerak, memperoleh perlakuan yang sama, serta terlindung dari

penangkapan sewenang-wenang dan gangguan terhadap kehidupan pribadi. Hak-hak ini bukan hadiah dari penguasa. Dalam negara hukum, ia merupakan batas yang mengikat pemegang kekuasaan sekaligus kewajiban negara untuk menghormati, melindungi, dan memenuhinya.

Kebebasan sipil juga mempunyai dimensi kelembagaan. Warga memerlukan pengadilan yang dapat diakses, pers yang bebas, parlemen yang menjalankan pengawasan, organisasi masyarakat sipil, lembaga audit, dan prosedur pengaduan. Tanpa institusi tersebut, hak di atas kertas sulit digunakan. Dalam ruang digital, dimensi kelembagaan bertambah kompleks karena komunikasi dan data dikuasai bersama oleh pemerintah, perusahaan platform, penyedia telekomunikasi, pengembang perangkat lunak, dan perantara data. Karena itu, perlindungan kebebasan tidak berhenti pada larangan negara menyensor; ia juga menuntut aturan yang mencegah platform atau kontraktor privat menjadi saluran pembatasan hak tanpa pertanggungjawaban.

Kebebasan berpendapat dan ruang kritik

Kebebasan berpendapat mempunyai dua lapis. Kebebasan memegang keyakinan atau opini tidak boleh dipaksa oleh negara. Kebebasan menyampaikan pendapat dapat dikenai pembatasan tertentu, tetapi pembatasan itu harus memenuhi syarat hukum hak asasi manusia. Komite HAM PBB menegaskan bahwa ekspresi menjadi dasar transparansi dan akuntabilitas, serta pembatasan harus dirumuskan secara jelas dan dibuktikan perlu bagi tujuan yang sah (Human Rights Committee, 2011). Ruang kritik mencakup kritik keras terhadap kebijakan, pejabat, partai, lembaga, dan keputusan publik; ketidaknyamanan penguasa terhadap kritik tidak dengan sendirinya menjadi alasan pembatasan.

Ruang kritik bukan ruang tanpa tanggung jawab. Ancaman kekerasan yang nyata, hasutan langsung yang memenuhi ambang hukum, penipuan, atau

pelanggaran hak orang lain dapat ditangani melalui proses yang adil. Namun, kritik kebijakan perlu dibedakan dari penghinaan, disinformasi, ancaman, dan ujaran kebencian dengan definisi yang presisi dan bukti yang kontekstual. Dalam komunikasi digital, satu potongan kalimat dapat tersebar tanpa konteks, sementara sindiran atau kritik satir bisa dibaca secara harfiah. Penegakan yang mengabaikan konteks berisiko menghasilkan efek gentar: warga memilih diam karena tidak mengetahui batas aman berbicara. Fenomena itu merugikan bukan hanya individu, melainkan juga mutu informasi yang diterima pemerintah.

Perubahan sifat komunikasi digital

Ruang digital memperluas akses warga untuk memproduksi dan menyebarkan informasi, membangun komunitas, mendokumentasikan peristiwa, dan mengawasi pejabat. Telepon pintar memungkinkan warga merekam pelayanan buruk atau dugaan kekerasan, sementara kanal pengaduan daring dapat mempertemukan masyarakat dengan institusi. Di sisi lain, kecepatan penyebaran, pencarian berbasis nama, pengarsipan permanen, penggabungan data, serta rekomendasi algoritmik membuat komunikasi digital memiliki konsekuensi jangka panjang. Unggahan yang semula ditujukan kepada lingkaran kecil dapat dipindahkan ke konteks politik yang luas, disimpan, diberi label, atau digunakan dalam keputusan yang tidak diketahui pengunggahnya.

Karakteristik tersebut mengubah hubungan antara ekspresi dan risiko. Pengawasan tidak perlu selalu hadir sebagai penyadapan langsung. Pengumpulan metadata komunikasi, riwayat lokasi, interaksi daring, pola perjalanan, dan hubungan sosial dapat membentuk profil perilaku. Kosta (2022) menunjukkan bahwa pengawasan algoritmik menantang asumsi hukum tradisional tentang siapa yang dapat dikenali sebagai korban karena pengelompokan dan prediksi dapat berlangsung tanpa sepengetahuan orang yang terdampak. Akibatnya, mekanisme pengaduan yang hanya mengandalkan individu mengetahui bahwa dirinya diawasi dapat tidak memadai. Desain

perlindungan perlu membuka ruang pengawasan kolektif, audit independen, dan pengujian sistem, bukan hanya pemulihan setelah kerugian terbukti.

Pemerintahan digital: manfaat dan risiko

Pemerintahan digital dapat memperbaiki akses layanan, mengurangi biaya administrasi, meningkatkan konsistensi, mendeteksi anomali transaksi, dan membantu pemerintah mengalokasikan sumber daya. Sistem registrasi sosial dapat mendukung penyaluran bantuan, rekam kesehatan dapat mempercepat kesinambungan perawatan, dan kanal digital dapat menyediakan informasi publik secara lebih luas. Manfaat tersebut tidak otomatis. Ia bergantung pada kualitas data, kemampuan warga menggunakan layanan, keamanan infrastruktur, interoperabilitas yang terkendali, serta adanya jalur layanan alternatif ketika sistem gagal atau seseorang tidak memiliki perangkat dan koneksi memadai.

Risiko muncul ketika infrastruktur yang dibangun untuk satu tujuan digunakan kembali bagi tujuan lain tanpa dasar hukum dan evaluasi baru. Data layanan kesehatan, pendidikan, bantuan sosial, dan administrasi kependudukan dapat menjadi sangat sensitif ketika digabungkan. Sistem yang salah mengklasifikasikan seseorang berpotensi memengaruhi akses layanan atau memicu pemeriksaan lebih lanjut. Ketergantungan pada vendor juga dapat mengaburkan tanggung jawab: instansi menyatakan sistem dikembangkan pihak ketiga, sementara vendor menganggap keputusan tetap berada pada pemerintah. Prinsip akuntabilitas menuntut bahwa keputusan yang berdampak pada hak tetap menjadi tanggung jawab pejabat publik, meskipun perangkat teknisnya dibeli dari perusahaan.

Keamanan publik dan kepentingan yang sah

Negara mempunyai kewajiban melindungi masyarakat dari ancaman serius, termasuk tindak pidana, kekerasan, terorisme, eksploitasi anak, serangan

terhadap infrastruktur penting, kebocoran data, dan bencana. Teknologi digital dapat membantu respons cepat, komunikasi krisis, analisis pola serangan, dan koordinasi antarinstansi. Penyelidikan berbasis data juga dapat menemukan hubungan yang sulit dideteksi secara manual. Mengakui manfaat ini penting agar perdebatan hak tidak menyederhanakan keamanan sebagai dalih semata. Warga yang menjadi korban kekerasan atau kejahatan digital juga berhak memperoleh perlindungan yang efektif.

Akan tetapi, konsep keamanan perlu dirinci. "Keamanan nasional" yang terlalu umum dapat menaungi kepentingan yang sangat berbeda, dari pencegahan serangan sampai pengelolaan kritik politik. Agar dapat diuji, kebijakan harus mengidentifikasi ancaman, kelompok risiko, tindakan yang diusulkan, dasar kewenangan, jangka waktu, serta cara mengukur hasil. Dalam analisis kebijakan, klaim bahwa pengumpulan data luas akan meningkatkan keamanan harus dibandingkan dengan bukti efektivitas dan risiko salah sasaran. Bellanova (2022) menunjukkan bahwa sistem keamanan algoritmik bergantung pada infrastruktur data yang menghubungkan aktor publik dan privat, sementara keputusan yang dihasilkan bisa tersebar dan sulit digugat. Pengawasan kebijakan harus mencakup keseluruhan rantai tersebut.

Uji pembatasan hak: legalitas, tujuan, kebutuhan, proporsionalitas

Kerangka hak asasi manusia menyediakan tes berlapis untuk menilai pembatasan kebebasan. Pertama, legalitas: pembatasan harus memiliki dasar hukum yang dapat diakses, cukup jelas, dapat diprediksi, dan mengandung perlindungan terhadap penyalahgunaan. Istilah yang kabur seperti "meresahkan", "mengganggu ketertiban" atau "menghina" perlu ditafsirkan secara ketat agar warga dapat mengetahui perilaku yang dilarang. Kedua, tujuan yang sah: negara perlu menunjukkan bahwa tindakan diarahkan pada kepentingan yang diakui, misalnya keselamatan publik atau perlindungan hak orang lain, bukan sekadar menghindari rasa malu atau menekan oposisi.

Ketiga, kebutuhan: harus ada kebutuhan sosial yang mendesak, bukti ancaman yang relevan, dan penjelasan mengapa tindakan tersebut dapat membantu. Keempat, proporsionalitas: dampak terhadap hak tidak boleh melebihi manfaat keamanan yang dapat dibuktikan. Kelima, tindakan harus menjadi pilihan yang paling ringan di antara alternatif yang sama efektifnya. Misalnya, penyelidikan terarah dengan otorisasi hakim dapat lebih proporsional daripada pemantauan menyeluruh terhadap seluruh pengguna. Pembatasan juga perlu dibatasi waktu, ruang lingkup, dan tujuan; disertai pencatatan akses, evaluasi berkala, serta mekanisme banding. Prinsip ini sejalan dengan penekanan Komite HAM PBB pada syarat hukum dan kebutuhan pembatasan ekspresi (Human Rights Committee, 2011).

Privasi sebagai prasyarat kebebasan

Privasi kerap dipahami sebagai kepentingan pribadi untuk menyembunyikan sesuatu. Pengertian ini terlalu sempit. Privasi memberi individu ruang untuk membentuk identitas, menjalin hubungan, mencari informasi sensitif, mempertimbangkan pilihan, dan mengubah pendapat tanpa terus-menerus dinilai oleh otoritas. Ia juga membatasi kemampuan pihak yang kuat untuk menggabungkan data dalam rangka memprediksi atau memengaruhi perilaku. Ketika seseorang merasa setiap pencarian, pertemuan, atau percakapan dapat diamati, ia mungkin menghindari kegiatan yang sah tetapi berisiko disalahpahami. Dengan demikian, privasi menopang kebebasan berbicara, berkumpul, beragama, dan berpartisipasi dalam politik (Nissenbaum, 2010; Lyon, 2018; Zuboff, 2019).

Perlindungan privasi digital memerlukan tata kelola sepanjang siklus data: pengumpulan, penggunaan, pertukaran, penyimpanan, pengamanan, dan penghapusan. Prinsip minimisasi data berarti pemerintah hanya mengumpulkan informasi yang relevan dan diperlukan. Pembatasan tujuan mencegah penggunaan ulang secara diam-diam. Retensi harus mempunyai batas yang

dapat dijelaskan; akses perlu dibatasi berdasarkan peran; pemindahan lintas instansi harus terekam; dan kebocoran harus ditangani dengan pemberitahuan serta mitigasi. UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan kerangka nasional untuk hak subjek data dan kewajiban pengendali/pemroses. Efektivitasnya bergantung pada aturan pelaksana, kapasitas pengawasan, penegakan yang konsisten, dan kemampuan warga memperoleh pemulihan.

Pengawasan digital dan efek gentar

Pengawasan mempunyai efek langsung dan tidak langsung. Efek langsung terjadi ketika data dipakai untuk mengidentifikasi seseorang, menghentikan suatu kegiatan, atau menolak layanan. Efek tidak langsung terjadi ketika persepsi bahwa seseorang selalu diawasi mendorong perubahan perilaku. Jurnalis mungkin mengurangi kontak dengan narasumber; aktivis menunda pertemuan; pegawai enggan mengkritik kebijakan; warga menghapus unggahan atau menghindari kelompok tertentu. Efek gentar sulit diukur karena tindakan yang tidak jadi dilakukan tidak tercatat. Namun, ketiadaan keluhan publik bukan bukti bahwa sistem tidak menekan kebebasan, sebab orang yang takut dapat memilih tidak mengadu.

Risiko tersebut meningkat ketika hukum tidak jelas, pengawasan dilakukan secara rahasia, dan warga tidak memiliki jalan untuk memeriksa atau memperbaiki data yang salah. Sistem prediktif dapat menghasilkan daftar risiko yang tampak objektif, padahal keputusan bergantung pada pemilihan indikator, kualitas data historis, definisi "anomali", dan ambang klasifikasi. Young, Katell, dan Krafft (2019) menekankan pentingnya inventarisasi teknologi, konsultasi publik, dan perangkat penilaian risiko agar komponen algoritmik lebih terlihat oleh pemangku kepentingan. Transparansi bukan tuntutan agar setiap kode sumber dipublikasikan tanpa pertimbangan keamanan; ia berarti publik dan

pengawas independen dapat mengetahui tujuan, dasar, dampak, prosedur koreksi, serta siapa yang bertanggung jawab.

Algoritma, kecerdasan buatan, dan akuntabilitas

Algoritma adalah rangkaian prosedur komputasional, sementara kecerdasan buatan mencakup beragam sistem yang melakukan tugas seperti pengenalan pola, klasifikasi, prediksi, atau generasi konten. Istilah-istilah ini tidak boleh digunakan sebagai kotak hitam yang membebaskan pemerintah dari kewajiban menjelaskan keputusan. Sistem dapat menggabungkan data administrasi, sinyal komunikasi, citra, dan model statistik. Kesalahan kecil dalam pencatatan dapat diperkuat ketika data dipakai untuk menentukan risiko. Bias historis juga dapat disalin ke dalam sistem baru, misalnya jika wilayah yang dahulu lebih sering diperiksa menjadi lebih sering ditandai sebagai berisiko karena datanya lebih banyak.

Akuntabilitas algoritmik perlu mencakup tujuan penggunaan, kategori data, tingkat akurasi pada kelompok berbeda, tingkat kesalahan positif dan negatif, proses validasi, perubahan model, sumber vendor, serta jalur keberatan. Penilaian dampak hak asasi manusia sebaiknya dilakukan sebelum pengadaan dan sepanjang penggunaan. Sistem yang memengaruhi kebebasan, akses bantuan, layanan kesehatan, atau proses hukum harus menjalani pengawasan lebih kuat daripada aplikasi informasi umum. Keputusan yang merugikan perlu ditinjau manusia yang memiliki kewenangan untuk membatalkan hasil mesin dan memberi alasan yang dapat dimengerti. Jika sistem tidak dapat diaudit atau tidak menunjukkan manfaat yang dapat dibuktikan, pemerintah perlu mempertimbangkan moratorium atau penghentian. Tuntutan proses yang adil juga penting ketika prediksi otomatis memengaruhi akses seseorang pada layanan atau keputusan publik (Citron & Pasquale, 2014).

Moderasi konten dan peran perusahaan platform

Pemerintah tidak mengendalikan seluruh ruang digital secara langsung. Perusahaan platform menetapkan aturan, menghapus konten, menurunkan jangkauan, menangguhkan akun, dan mengelola sistem rekomendasi. Keputusan tersebut dapat memengaruhi akses publik terhadap informasi dan kesempatan warga untuk menyampaikan kritik. Moderasi diperlukan untuk mengatasi ancaman, eksploitasi, penipuan, dan konten yang melanggar hukum. Namun, jika tekanan pemerintah berlangsung secara informal atau tidak terdokumentasi, platform dapat membatasi ekspresi lebih luas untuk menghindari risiko hukum atau bisnis. Kondisi ini menciptakan "sensor melalui perantara" tanpa prosedur yang mudah diketahui pengguna.

Tata kelola moderasi perlu membedakan perintah hukum formal dari permintaan sukarela, menyediakan alasan yang spesifik, memberi pemberitahuan kepada pengguna jika memungkinkan, membuka kanal banding, serta menerbitkan laporan transparansi yang dapat diperiksa. Dalam keadaan mendesak, tindakan sementara dapat diperlukan, tetapi harus ditinjau kembali dalam waktu singkat dan tunduk pada evaluasi setelah kejadian. Pengguna juga seharusnya dapat mengetahui apakah jangkauan kontennya dibatasi oleh sistem rekomendasi atau tindakan moderasi. Kerangka konstitusional untuk moderasi daring mengingatkan bahwa hak berekspresi juga berhubungan dengan cara informasi disusun dan disalurkan oleh platform, bukan hanya dengan larangan formal negara (Kuczerawy, 2020).

Kerangka hukum Indonesia

UUD Negara Republik Indonesia Tahun 1945 menjamin kebebasan menyatakan pikiran dan sikap, mengeluarkan pendapat, memperoleh informasi, berkomunikasi, serta perlindungan diri dan rasa aman, antara lain dalam Pasal 28E, 28F, dan 28G. Pasal 28J menyatakan bahwa pelaksanaan hak dapat dibatasi

dengan undang-undang untuk tujuan yang ditentukan, termasuk penghormatan hak orang lain, moral, keamanan, dan ketertiban umum dalam masyarakat demokratis. Struktur ini menuntut pembacaan seimbang: negara berkewajiban melindungi hak sekaligus menjelaskan secara ketat pembatasan yang dipilih. Pembatasan tidak cukup dibenarkan hanya dengan menyebut ketertiban atau keamanan tanpa menunjukkan kebutuhan dan proporsionalitasnya.

Indonesia mengesahkan Kovenan Internasional tentang Hak-Hak Sipil dan Politik melalui UU Nomor 12 Tahun 2005. UU Nomor 27 Tahun 2022 mengatur pelindungan data pribadi. Perubahan kedua UU Informasi dan Transaksi Elektronik melalui UU Nomor 1 Tahun 2024 menyatakan adanya kebutuhan memperbaiki ketentuan yang dalam pelaksanaannya menimbulkan multitafsir dan kontroversi (Indonesia, 2024). Hal ini menunjukkan bahwa kualitas rumusan dan praktik penegakan merupakan bagian dari problem kebijakan, bukan isu teknis belaka. Penilaian hukum konkret harus merujuk naskah resmi, putusan pengadilan, dan peraturan pelaksana yang berlaku. Artikel ini menyajikan kerangka analitis, bukan pendapat hukum atas perkara tertentu.

Menjaga agar hukum tidak membungkam kritik

Perumusan tindak pidana digital harus menghindari istilah yang terlalu luas dan memberi bobot pada konteks, maksud, jangkauan, serta dampak nyata. Kritik terhadap penyelenggara negara, pejabat publik, dan kebijakan perlu memperoleh perlindungan yang memadai karena akuntabilitas publik menuntut kemungkinan menguji klaim dan keputusan mereka. Namun, perlindungan terhadap kritik tidak berarti mengabaikan ancaman serius atau kampanye pelecehan yang menargetkan seseorang. Pembedaan perlu dilakukan dengan standar bukti, bukan dengan preferensi politik penegak hukum. Penggunaan mediasi, hak jawab, koreksi, atau ganti rugi perdata dapat lebih sesuai daripada

pidana untuk sengketa tertentu, bergantung pada sifat perbuatan dan hukum yang berlaku.

Praktik penegakan juga harus konsisten. Laporan warga tidak boleh diperlakukan berbeda hanya karena mengkritik aktor yang memiliki kekuasaan. Pedoman penuntutan dapat menjelaskan unsur, standar pembuktian, dan pertimbangan kepentingan publik; statistik perkara dapat diterbitkan dengan perlindungan data pribadi; serta keputusan penghentian atau penerusan perkara dapat diaudit. Pelatihan bagi penyidik, jaksa, hakim, pejabat komunikasi, dan pengelola platform perlu memasukkan literasi digital serta standar hak asasi. Perlindungan terhadap pelapor pelanggaran, jurnalis, akademisi, dan pembela HAM harus dirancang agar warga dapat mengungkap masalah tanpa menghadapi intimidasi atau pembalasan yang tidak sah.

Transparansi, pengawasan, dan pemulihan

Pengawasan yang efektif harus independen dari unit yang mengoperasikan teknologi. Parlemen dapat meminta laporan penggunaan sistem dan alasan kebijakan; lembaga audit memeriksa kontrak, keamanan, dan kepatuhan; pengadilan memberi otorisasi atau menilai sengketa; komisi independen memeriksa perlindungan data dan hak; sementara masyarakat sipil serta universitas menilai dampak sosial. Fungsi-fungsi ini tidak harus terpusat pada satu lembaga, tetapi mandat, akses informasi, dan perlindungan independensinya harus jelas. Untuk sistem yang bersifat rahasia, pengawasan dapat dilakukan oleh badan berwenang yang mempunyai akses aman, dengan ringkasan hasil yang dapat dipublikasikan.

Pemulihan harus praktis dan tepat waktu. Seseorang yang dirugikan perlu dapat mengetahui keputusan yang memengaruhi dirinya, meminta koreksi data, mengajukan keberatan, memperoleh peninjauan manusia, dan meminta kompensasi atau pemulihan sesuai hukum. Dalam kasus pengawasan rahasia,

pemberitahuan setelah risiko penyelidikan berlalu dapat menjadi salah satu pilihan, disertai mekanisme pengaduan yang tidak mewajibkan korban membuktikan hal yang memang tidak dapat diketahuinya. Tanpa pemulihan, transparansi hanya menghasilkan pengetahuan tentang pelanggaran tanpa konsekuensi. Tanpa konsekuensi, insentif untuk mematuhi batas hukum menjadi lemah.

Keamanan siber tanpa pengawasan berlebihan

Keamanan siber merupakan bagian nyata dari keamanan publik. Pemerintah mengelola data sensitif dan layanan penting, sehingga perlu melindungi jaringan dari pencurian, sabotase, ransomware, penyalahgunaan kredensial, dan manipulasi informasi. Langkah pertahanan yang baik meliputi enkripsi, autentikasi berlapis, pembaruan sistem, pencadangan, segmentasi jaringan, respons insiden, pengujian keamanan, dan pelatihan pegawai. Praktik ini berfokus pada ketahanan sistem, bukan pemantauan menyeluruh atas ekspresi masyarakat. Keamanan yang dirancang dengan minimisasi data sering kali sekaligus mengurangi dampak kebocoran dan potensi penyalahgunaan.

Perlu pula dibedakan antara pengamanan infrastruktur dan pengawasan isi komunikasi. Pemerintah dapat memantau lalu lintas jaringan untuk mendeteksi serangan dengan pembatasan tujuan, retensi minimum, kontrol akses, dan audit. Pemantauan semacam itu tidak boleh berubah menjadi pengumpulan konten dan metadata tanpa dasar yang relevan. Program keamanan harus menilai risiko penyalahgunaan internal, karena pegawai berwenang dapat mengakses informasi melebihi kebutuhan tugas. Prinsip least privilege, pemisahan tugas, pencatatan akses, pemeriksaan berkala, dan sanksi atas akses ilegal membantu menjaga integritas. Keamanan yang baik membatasi kemampuan penyerang sekaligus mengurangi kesempatan penyalahgunaan oleh institusi sendiri.

Keterbukaan pemerintah sebagai sumber keamanan demokratis

Keterbukaan sering dianggap berlawanan dengan keamanan, padahal informasi yang dapat diuji publik dapat memperkuat kepercayaan dan membantu menemukan kerentanan kebijakan. Pemerintah dapat menjelaskan tujuan program, dasar hukum, kategori teknologi, prosedur pengawasan, jumlah permintaan data, dan hasil evaluasi tanpa membuka rincian operasional yang dapat membahayakan penyelidikan. Pengungkapan bertingkat memungkinkan publik mendapat informasi agregat, sedangkan pengawas berwenang mengakses rincian sensitif. Laporan yang teratur membuat perubahan praktik terlihat dan membantu pembuat kebijakan membandingkan manfaat dengan biaya hak.

Partisipasi publik juga memperbaiki kualitas desain. Konsultasi sebelum pengadaan dapat mengungkap persoalan yang tidak terlihat oleh pengembang, misalnya dampak pada kelompok adat, minoritas bahasa, anak, penyandang disabilitas, pekerja informal, atau warga yang tidak memiliki dokumen lengkap. Partisipasi bukan sekadar sosialisasi keputusan yang sudah diambil. Ia memerlukan waktu, bahan teknis yang dapat dipahami, kesempatan mengajukan alternatif, dan jawaban atas masukan. Young et al. (2019) menunjukkan bahwa proses keterlibatan publik dan pengungkapan teknologi merupakan komponen penting dalam regulasi pengawasan tingkat kota. Prinsip itu dapat disesuaikan dalam konteks Indonesia melalui forum konsultasi, uji dampak, dan kanal pengaduan yang terhubung dengan proses pengambilan keputusan.

Keadilan digital dan kelompok rentan

Dampak pengawasan dan pembatasan ekspresi tidak terbagi merata. Kelompok minoritas, masyarakat adat, aktivis, jurnalis, oposisi politik, pekerja platform, migran, dan warga miskin dapat lebih sering menjadi objek pemeriksaan atau

mengalami kesulitan membantah klasifikasi. Kesenjangan akses digital menambah masalah: layanan yang hanya tersedia daring dapat mengecualikan orang tanpa perangkat, koneksi, kemampuan baca digital, atau dokumen formal. Jika data historis mencerminkan ketimpangan, sistem otomatis dapat mengulangnya dalam skala lebih besar. Karena itu, audit harus memeriksa hasil yang terpilah, bukan hanya angka akurasi rata-rata.

Keadilan menghendaki proses desain yang mengikutsertakan pihak terdampak dan menyediakan akomodasi. Misalnya, sistem deteksi kecurangan bantuan sosial harus mempunyai mekanisme klarifikasi yang mudah diakses, bukan hanya notifikasi elektronik yang sulit dipahami. Identitas digital perlu didukung prosedur pemulihan jika seseorang kehilangan perangkat atau datanya keliru. Pengujian juga harus memperhitungkan dialek, variasi nama, alamat tidak baku, dan praktik kehidupan masyarakat setempat. Tujuannya bukan menolak otomatisasi, tetapi memastikan bahwa efisiensi tidak dicapai dengan mengalihkan beban kesalahan kepada warga yang paling sedikit memiliki daya tawar.

Disinformasi, moderasi, dan ketahanan publik

Informasi palsu yang terkoordinasi dapat mengganggu kesehatan masyarakat, pemilu, keamanan komunitas, dan kepercayaan terhadap institusi. Respons negara diperlukan ketika ada penipuan atau ancaman nyata. Namun, kebijakan melawan disinformasi dapat menjadi alat sensor apabila "kebenaran resmi" ditentukan tanpa proses terbuka atau jika kritik yang tidak populer langsung diperlakukan sebagai ancaman. Pemerintah sendiri dapat keliru, sementara bukti ilmiah berkembang. Karena itu, respons harus membedakan konten yang terbukti palsu dan berbahaya dari pendapat, interpretasi, satire, atau laporan awal yang masih diverifikasi.

Pendekatan yang berkelanjutan mencakup keterbukaan data, klarifikasi cepat, literasi media, kerja sama dengan jurnalis dan ahli independen, serta penindakan yang terarah terhadap pelaku penipuan atau ancaman. Penghapusan konten sebaiknya menjadi langkah yang terukur, disertai alasan, bukti, hak banding, dan pengawasan. Label koreksi atau konteks dapat lebih sesuai daripada penghapusan total dalam sejumlah keadaan. Negara harus menerapkan standar yang sama pada komunikasinya sendiri: informasi pemerintah yang salah perlu dikoreksi secara terbuka. Ketahanan publik tumbuh dari kepercayaan yang dapat diuji, bukan dari upaya memonopoli narasi.

Desain kebijakan: dari prinsip ke prosedur

Prinsip hak asasi perlu diterjemahkan menjadi prosedur kerja instansi. Sebelum teknologi digunakan, unit pemilik kebijakan menyusun tujuan yang terukur, dasar kewenangan, peta data, analisis ancaman, penilaian dampak hak, alternatif non-digital, serta rencana penghentian. Pengadaan mencantumkan klausul audit, keamanan, interoperabilitas, larangan penggunaan ulang, akses terhadap dokumentasi, penghapusan data, dan pembagian tanggung jawab. Uji coba harus dibatasi ruang dan waktu, melibatkan kelompok terdampak, dan tidak otomatis menjadi penggunaan nasional tanpa evaluasi independen.

Selama operasi, instansi mencatat akses, perubahan model, permintaan pihak lain, kesalahan, dan keluhan. Evaluasi berkala mengukur manfaat yang benar-benar dihasilkan serta kerugian dan ketimpangan yang terjadi. Jika sistem gagal memenuhi ambang yang ditetapkan, penggunaan dihentikan atau diperbaiki. Pengawasan harus melihat perjalanan data dan keputusan, bukan hanya antarmuka yang tampak kepada pengguna. Kerangka ini memungkinkan organisasi menerapkan inovasi sambil mempertahankan tanggung jawab yang dapat ditelusuri. Dalam logika manajemen, tata kelola hak dapat diperlakukan sebagai bagian dari manajemen risiko dan mutu layanan, bukan hambatan eksternal setelah proyek selesai.

Agenda kebijakan bagi Indonesia

Pertama, pemerintah perlu memperkuat inventaris nasional dan sektoral atas sistem digital berisiko tinggi, termasuk tujuan, pemilik, vendor, jenis data, dasar hukum, dan jalur pengaduannya. Kedua, penilaian dampak hak asasi dan privasi perlu menjadi persyaratan sebelum pengadaan sistem yang memantau, memprofilkan, atau memengaruhi hak. Ketiga, lembaga pengawasan harus memperoleh sumber daya, akses aman, dan independensi yang cukup. Keempat, aturan penegakan ekspresi digital perlu memberi kepastian yang lebih tinggi serta perlindungan khusus bagi kritik kepentingan publik. Kelima, layanan publik digital harus mempunyai jalur alternatif yang layak dan aksesibel.

Keenam, kontrak pemerintah dengan penyedia teknologi perlu mengatur penggunaan data, audit, keamanan, interoperabilitas, pembaruan sistem, dan penghentian layanan. Ketujuh, statistik penegakan hukum, permintaan data, pemblokiran konten, dan insiden kebocoran sebaiknya dilaporkan secara agregat dan teratur. Kedelapan, literasi digital perlu mengajarkan bukan hanya cara memakai aplikasi, melainkan juga hak, keamanan akun, verifikasi informasi, pengaduan, dan pemahaman dasar tentang algoritma. Kesembilan, kerja sama regional dan internasional harus mempertimbangkan aliran data lintas batas serta perlindungan hak yang setara. Agenda ini tidak mengharuskan Indonesia menyalin model negara lain; ia memberi ukuran agar inovasi disesuaikan dengan konstitusi, kapasitas, dan keragaman sosial nasional.

Implikasi bagi pendidikan, manajemen, dan riset

Perguruan tinggi dapat menjadikan tata kelola digital sebagai materi lintas disiplin. Mahasiswa manajemen perlu memahami bahwa transformasi digital menyentuh kepercayaan, legitimasi, risiko reputasi, kepatuhan, dan kualitas pelayanan; mahasiswa teknologi perlu memahami bahwa desain sistem memuat pilihan nilai; sementara mahasiswa hukum dan kebijakan publik perlu mengenali

batas teknis sistem yang mereka atur. Studi kasus dapat meminta mahasiswa membandingkan manfaat program pengawasan tertentu dengan alternatif yang kurang intrusif, lalu menerapkan uji legalitas dan proporsionalitas. Latihan demikian mengembangkan penilaian, bukan sekadar hafalan istilah.

Agenda riset Indonesia dapat mencakup pengalaman warga menghadapi layanan otomatis, dampak penegakan hukum digital terhadap perilaku berbicara, efektivitas mekanisme koreksi data, tata kelola vendor, kesenjangan dampak algoritma, dan kualitas konsultasi publik. Riset kualitatif dapat menelusuri bagaimana warga memahami risiko pengawasan; riset kuantitatif dapat menguji kaitan antara kepercayaan, transparansi, dan partisipasi; analisis kebijakan dapat membandingkan prosedur antarsektor. Peneliti perlu melindungi subjek penelitian, terutama ketika topik berhubungan dengan kritik pemerintah atau pengawasan. Metode yang bertanggung jawab sama pentingnya dengan pertanyaan yang relevan.

Kerangka evaluasi bagi organisasi publik

Organisasi publik dapat menilai program digital melalui beberapa pertanyaan. Apakah tujuan dan dasar hukumnya jelas? Apakah data yang dikumpulkan memang diperlukan? Siapa yang dapat mengaksesnya dan berapa lama data disimpan? Apakah kelompok yang berpotensi dirugikan telah diajak menilai dampak? Dapatkah warga meminta penjelasan dan koreksi? Apakah ada peninjauan manusia yang kompeten? Apakah efektivitas keamanan diukur dengan indikator yang relevan, dan dibandingkan dengan alternatif? Apakah terdapat rencana penghentian, penanganan insiden, serta audit independen? Pertanyaan ini dapat menjadi bagian dari gerbang keputusan dalam siklus hidup proyek.

Indikator evaluasi sebaiknya mencakup kinerja layanan, tingkat kesalahan, distribusi manfaat dan beban, keluhan, waktu penyelesaian banding,

aksesibilitas, insiden keamanan, dan kepatuhan pada batas retensi. Keberhasilan tidak cukup dinilai dari jumlah data yang diproses atau kecepatan sistem. Program yang cepat tetapi sering menolak warga secara keliru dapat meningkatkan biaya sosial dan mengurangi kepercayaan. Pengukuran juga perlu membedakan korelasi dari dampak kausal: apabila kriminalitas menurun setelah teknologi dipakai, perlu diteliti apakah penurunan itu benar-benar disebabkan sistem atau dipengaruhi faktor lain. Evaluasi berbasis bukti melindungi hak sekaligus mengurangi investasi pada teknologi yang tidak efektif.

Keadaan darurat dan batas waktu kekuasaan digital

Keadaan darurat dapat memerlukan koordinasi cepat, pembatasan mobilitas, atau pengumpulan informasi untuk mencegah bahaya langsung. Namun, keadaan darurat juga meningkatkan risiko normalisasi kewenangan luar biasa. Langkah yang semula dipakai untuk waktu singkat dapat dipertahankan karena sistem, kontrak, dan basis datanya sudah tersedia. Karena itu, setiap kebijakan darurat perlu menetapkan pemicu yang dapat diverifikasi, cakupan kewenangan, kelompok yang terdampak, batas waktu, dan prosedur pencabutan. Perpanjangan harus didasarkan pada penilaian baru, bukan semata-mata pada alasan bahwa teknologi telah terlanjur diadakan. Pengawasan legislatif dan yudisial tetap relevan, sekalipun tata cara pemeriksaannya disesuaikan agar tidak membocorkan informasi operasional yang sensitif.

Klausul kedaluwarsa dapat mencegah kewenangan darurat berubah menjadi kewenangan permanen. Pada akhir masa berlaku, instansi perlu melaporkan apa yang dilakukan, ancaman yang dihadapi, efektivitas langkah, kesalahan yang terjadi, serta data apa yang masih disimpan. Data yang tidak lagi diperlukan harus dihapus atau dianonimkan secara dapat diverifikasi. Publikasi laporan pascakejadian membantu masyarakat menilai apakah tindakan pemerintah proporsional. Jika terjadi pelanggaran, mekanisme pemulihan harus tetap terbuka. Kecepatan pada saat krisis dapat dibenarkan secara operasional, tetapi

tidak menghapus kewajiban untuk memberi alasan dan memperbaiki kerugian setelah keadaan mendesak berlalu.

Pers dan masyarakat sipil sebagai infrastruktur pengawasan

Jurnalisme independen dan organisasi masyarakat sipil menjalankan fungsi pengawasan yang tidak dapat sepenuhnya digantikan oleh audit internal. Pers dapat menguji klaim resmi, menelusuri pengadaan, mengungkap pola dampak, dan menyampaikan pengalaman kelompok yang tidak terdengar dalam forum kebijakan. Organisasi masyarakat sipil dapat membantu warga memahami prosedur, mengajukan permintaan informasi, serta mengidentifikasi kesenjangan antara aturan dan praktik. Peran ini bergantung pada akses terhadap dokumen publik, perlindungan sumber, kebebasan berkumpul, dan kemampuan bekerja tanpa intimidasi. Karena itu, kebebasan pers dan ruang organisasi bukan tambahan bagi tata kelola digital; keduanya merupakan bagian dari sistem peringatan dini demokratis.

Kegiatan pengawasan harus dilakukan dengan standar etis. Peneliti dan jurnalis perlu melindungi data pribadi yang tidak relevan, memverifikasi bukti, memberi kesempatan tanggapan kepada pihak yang dituduh, dan menghindari publikasi rincian teknis yang secara nyata mempermudah serangan siber. Pemerintah dapat merespons temuan dengan menyediakan kanal koordinasi dan dokumen penjelas, bukan dengan menyamakan kritik dengan ancaman. Ketika kritik terbukti keliru, koreksi terbuka memberi ruang bagi pembelajaran publik. Ketika kritik benar, tindak lanjut yang dapat dilacak menunjukkan bahwa partisipasi memiliki akibat nyata. Hubungan ini memperkuat kepercayaan melalui akuntabilitas, bukan melalui tuntutan kepatuhan tanpa pemeriksaan.

Kemampuan administrasi dan etika pengadaan

Aturan yang baik tidak cukup jika instansi tidak memiliki kapasitas untuk menerapkannya. Pegawai yang merancang layanan digital perlu memahami

klasifikasi data, risiko keamanan, hak subjek data, aksesibilitas, dan dokumentasi keputusan. Pimpinan perlu memastikan tanggung jawab tidak terpecah antara unit teknologi, hukum, pengadaan, keamanan informasi, dan pelayanan publik. Sebuah komite tata kelola lintas fungsi dapat menilai sistem berisiko tinggi, menetapkan pemilik risiko, dan menyepakati kondisi penggunaan. Pelatihan perlu berbasis skenario: bagaimana menangani data keliru, permintaan akses, insiden kebocoran, keberatan warga, atau permintaan informal dari pejabat lain.

Pengadaan teknologi merupakan titik penting karena pilihan vendor dapat membentuk pilihan kebijakan selama bertahun-tahun. Kontrak seharusnya memberi pemerintah dan pengawas hak untuk memeriksa sistem, mendokumentasikan perubahan, menguji klaim performa, dan memastikan data dapat dihapus ketika hubungan berakhir. Pemerintah juga harus menilai risiko ketergantungan, termasuk apakah sistem dapat dipindahkan atau dihentikan tanpa kehilangan layanan publik. Spesifikasi yang hanya mengukur harga dan kecepatan dapat mengabaikan biaya sosial ketika terjadi kesalahan. Dengan memasukkan perlindungan hak, audit, interoperabilitas, dan aksesibilitas sebagai kriteria pengadaan, negara mengubah nilai publik menjadi persyaratan operasional yang dapat diperiksa.

Ukuran keberhasilan yang memasukkan kepercayaan

Keberhasilan pemerintahan digital biasanya diukur melalui waktu layanan, biaya per transaksi, jumlah pengguna, atau pengurangan antrean. Indikator itu penting, tetapi belum menjawab apakah warga merasa aman menyampaikan data, apakah kelompok tertentu lebih sering ditolak, atau apakah kritik terhadap layanan dapat disampaikan tanpa takut. Survei kepercayaan, tingkat penyelesaian pengaduan, jumlah koreksi data, perbedaan tingkat kesalahan antar kelompok, jumlah akses tidak sah, serta ketersediaan jalur layanan luring dapat melengkapi ukuran operasional. Indikator perlu dipilih sesuai konteks dan tidak dijadikan skor tunggal yang menyembunyikan variasi dampak.

Kepercayaan bukan hasil komunikasi publik semata. Ia terbentuk dari pengalaman warga bahwa data mereka digunakan sesuai tujuan, kesalahan diakui, keputusan dapat ditinjau, dan keluhan memperoleh jawaban. Pemerintah dapat mengukur kepercayaan dari waktu ke waktu, tetapi harus menjelaskan metode dan keterbatasan pengukuran. Jika kepercayaan turun, respons yang tepat bukan menganggap warga kurang paham, melainkan menyelidiki apakah penyebabnya adalah kebocoran, ketidakadilan, prosedur yang rumit, atau kurangnya penjelasan. Dengan menjadikan kepercayaan dan hak sebagai bagian dari kinerja, organisasi menghindari definisi efisiensi yang hanya melihat keluaran administratif.

Ilustrasi penerapan: analitik untuk mencegah penipuan bantuan

Bayangkan sebuah pemerintah daerah memakai analitik untuk menemukan klaim bantuan sosial yang diduga ganda. Sistem mencocokkan identitas, alamat, dan pola pembayaran, lalu menghasilkan daftar kasus untuk diperiksa petugas. Tujuan pencegahan penipuan merupakan kepentingan publik yang sah, tetapi daftar hasil algoritma bukan bukti kesalahan. Perbedaan ejaan nama, perpindahan tempat tinggal, keterbatasan dokumen, atau anggota keluarga dengan identitas serupa dapat menghasilkan kecocokan keliru. Jika bantuan dihentikan otomatis, warga dapat kehilangan akses kebutuhan dasar tanpa pernah mengetahui alasan keputusan. Sistem yang semula dimaksudkan untuk meningkatkan integritas program justru dapat memindahkan beban pembuktian kepada masyarakat yang paling rentan.

Penerapan yang lebih dapat dipertanggungjawabkan menggunakan hasil analitik sebagai sinyal untuk pemeriksaan, bukan keputusan akhir. Warga diberi pemberitahuan yang mudah dipahami, akses untuk mengoreksi data, kesempatan menyampaikan bukti, dan layanan banding yang tidak bergantung pada aplikasi tunggal. Petugas memeriksa kasus dengan prosedur seragam serta mencatat alasan menerima atau menolak rekomendasi sistem. Instansi menilai

tingkat kesalahan menurut wilayah dan kelompok, membatasi akses data, menghapus data yang tak lagi diperlukan, serta menguji apakah sistem benar-benar menemukan penipuan lebih baik daripada audit berbasis sampel. Ilustrasi ini menunjukkan bahwa prinsip hak dapat memperbaiki ketepatan kebijakan: koreksi data dan peninjauan manusia bukan sekadar perlindungan individual, tetapi cara mengurangi keputusan salah dan menjaga legitimasi layanan.

Sintesis: keamanan yang dibatasi menjadi lebih sah

Keamanan dan kebebasan sipil saling berhubungan melalui mutu institusi. Pengawasan yang sah dapat membantu menghadapi ancaman tertentu; pengawasan tanpa batas dapat merusak kepercayaan, membungkam kritik, dan mengurangi kualitas informasi yang dibutuhkan pemerintah untuk memperbaiki kebijakan. Kebebasan kritik juga mempunyai nilai praktis: ia memungkinkan warga dan media mengungkap kesalahan, menguji klaim, dan memberi peringatan sebelum risiko membesar. Karena itu, kebebasan bukan sekadar biaya yang harus ditoleransi demi keamanan, melainkan salah satu mekanisme yang membuat keamanan dapat dipertanggungjawabkan.

Pemerintahan digital yang demokratis harus mampu menjelaskan apa yang dikumpulkan, untuk tujuan apa, berdasarkan kewenangan mana, dalam jangka waktu berapa lama, dengan siapa data dibagikan, dan bagaimana keputusan dapat digugat. Ketika ancaman muncul, respons negara harus terarah, berbasis bukti, dan dapat ditinjau. Ketika sistem menghasilkan kesalahan, warga harus dapat memperoleh koreksi. Ketika kritik muncul, pemerintah perlu menanggapinya dengan informasi dan alasan, bukan dengan intimidasi. Dengan cara itu, teknologi digital memperkuat kapasitas negara tanpa mengubah warga menjadi objek yang terus-menerus dinilai.

Refleksi dan diskusi

Pembaca dapat menggunakan empat pertanyaan untuk menilai kebijakan pemerintahan digital di lingkungannya. Apakah tujuan sistem dinyatakan secara spesifik dan didukung bukti? Apakah warga mengetahui data apa yang dipakai dan dapat membetulkan kesalahan? Apakah pembatasan ekspresi atau pemantauan mempunyai batas waktu serta jalur keberatan? Siapa yang mengawasi ketika keputusan dibuat bersama oleh instansi dan perusahaan teknologi? Pertanyaan tersebut membantu menggeser diskusi dari klaim umum tentang modernisasi menuju pemeriksaan proses, dampak, dan tanggung jawab.

Diskusi kelas atau forum kebijakan dapat membandingkan dua pilihan: pengawasan luas yang menjanjikan deteksi dini dengan risiko dampak menyeluruh, dan penyelidikan terarah yang memerlukan bukti serta otorisasi lebih kuat. Peserta dapat mengidentifikasi siapa yang memperoleh manfaat, siapa yang menanggung kesalahan, dan informasi apa yang diperlukan untuk menilai efektivitas. Kasus bantuan sosial dalam artikel ini dapat dikembangkan dengan meminta mahasiswa merancang mekanisme banding, indikator kinerja, dan syarat penghentian sistem. Latihan itu memperlihatkan bahwa perlindungan hak tidak mengakhiri inovasi; ia menuntut inovasi dibuktikan, diarahkan, dan dikoreksi.

Kesimpulan

Kebebasan sipil, keamanan, dan ruang kritik merupakan unsur yang harus dirancang bersama dalam pemerintahan digital. Transformasi digital membuka peluang untuk layanan yang lebih cepat dan respons keamanan yang lebih baik, tetapi kemampuan menghubungkan data, membuat profil, serta memengaruhi informasi juga menambah risiko bagi privasi, ekspresi, dan kesetaraan. Risiko tersebut tidak hanya berasal dari niat buruk; ia dapat muncul dari rumusan

hukum yang kabur, tujuan yang melebar, data yang salah, ketergantungan vendor, dan sistem yang sulit digugat.

Ukuran utama tata kelola yang baik ialah apakah kekuasaan digital dapat dijelaskan, dibatasi, diperiksa, dan dipulihkan dampaknya. Legalitas, tujuan sah, kebutuhan, proporsionalitas, transparansi, pengawasan independen, keamanan data, partisipasi, dan mekanisme pemulihan perlu tertanam sejak tahap perencanaan sampai penghentian sistem. Untuk Indonesia, kerangka konstitusi dan peraturan yang telah ada harus diwujudkan melalui prosedur yang dapat dilaksanakan, lembaga pengawas yang efektif, dan praktik penegakan yang melindungi kritik kepentingan publik. Pemerintahan yang kuat bukan pemerintahan yang mengetahui segalanya tentang warga, melainkan pemerintahan yang mampu melindungi masyarakat sambil tunduk pada aturan dan koreksi demokratis.

Glossarium

Akuntabilitas algoritmik. Kewajiban menjelaskan, mengaudit, dan memperbaiki sistem algoritmik serta keputusan yang didukungnya.

Efek gentar (chilling effect). Perubahan perilaku berupa pembatasan ekspresi atau partisipasi yang sah karena takut diawasi atau dikenai sanksi.

Kebebasan sipil. Hak yang melindungi otonomi, partisipasi, dan ruang hidup warga dari campur tangan sewenang-wenang.

Minimisasi data. Prinsip mengumpulkan dan menggunakan hanya data yang relevan serta diperlukan untuk tujuan yang dinyatakan.

Moderasi konten. Proses platform menilai, menghapus, memberi label, atau membatasi distribusi konten dan akun.

Pengawasan digital. Pengumpulan dan analisis jejak digital untuk memantau, mengelola, atau memengaruhi individu/kelompok.

Proporsionalitas. Keharusan agar dampak pembatasan hak tidak berlebihan dibanding manfaat yang dituju.

Ruang kritik. Kondisi hukum dan sosial yang memungkinkan warga menguji keputusan, kebijakan, dan tindakan pemegang kekuasaan.

Tujuan pembatasan yang sah. Kepentingan yang diakui hukum HAM sebagai dasar pembatasan tertentu, misalnya keselamatan publik atau hak orang lain.

Uji kebutuhan. Penilaian apakah pembatasan menjawab kebutuhan sosial yang mendesak dan didukung alasan serta bukti yang relevan.

Daftar Pustaka

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. Regulation & Governance, 16(1), 102–118. https://doi.org/10.1111/rego.12338

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/

Human Rights Committee. (2011). General comment No. 34: Article 19: Freedoms of opinion and expression (CCPR/C/GC/34). United Nations. https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/gc34.pdf

Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Indonesia. (2005). Undang-Undang Republik Indonesia Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional tentang Hak-Hak Sipil dan Politik).

Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://jdih.komdigi.go.id/produk_hukum/view/id/832

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://jdih.komdigi.go.id/produk_hukum/view/id/884

Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. Regulation & Governance, 16(1), 212–224. https://doi.org/10.1111/rego.12331

Kuczerawy, A. (2020). Democratising online content moderation: A constitutional framework. Computer Law & Security Review, 36, 105374. https://doi.org/10.1016/j.clsr.2019.105374

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

United Nations. (2016). The promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/32/13). https://digitallibrary.un.org/record/845727/files/A_HRC_RES_32_13-EN.pdf

United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Young, M., Katell, M., & Krafft, P. M. (2019). Municipal surveillance regulation and algorithmic accountability. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719868492

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.