CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

ANTARA KEPENTINGAN PUBLIK DAN HAK ASASI: ANALISIS HUKUM TERHADAP PENGAWASAN NEGARA ATAS RUANG DIGITAL

Rivo Denra Maulana[1]

Email: 2210611458@mahasiswa.upnvj.ac.id

Universitas Pembangunan Nasional "Veteran" Jakarta

Abstrack

The advancement of information technology has expanded the state's capacity to conduct digital surveillance, including through data collection, electronic interception, and monitoring of online activity. While such surveillance is often justified on grounds of public interest—such as national security and public order—it simultaneously poses significant risks to human rights, particularly the rights to privacy and freedom of expression. This study aims to analyze the forms and limits of state authority in digital surveillance under Indonesia's national legal framework, as well as to formulate an ideal accountability mechanism to prevent surveillance from becoming repressive. Utilizing a normative juridical approach and qualitative analysis of legislation, Constitutional Court decisions, and scholarly literature, this research finds that state surveillance must adhere to the principles of legality, legitimate aim, necessity, and proportionality. The study further emphasizes the need to strengthen oversight mechanisms through independent judicial authorization, public transparency, multilayered supervision, and an independent data protection authority. The findings demonstrate that developing a comprehensive and human-rights-based digital surveillance regulatory framework is essential to maintaining a balanced relationship between public interest and the protection of human rights in Indonesia.

Keywords: ***digital surveillance, human rights, privacy, rule of law, accountability.***

Abstrak

Perkembangan teknologi informasi telah memperluas kemampuan negara dalam melakukan pengawasan digital, termasuk melalui pengumpulan data, penyadapan elektronik, dan pemantauan aktivitas daring. Meskipun pengawasan ini kerap dibenarkan untuk kepentingan publik seperti keamanan nasional dan ketertiban umum, praktik

Article History
Received: November 2025
Reviewed: November 2025
Published: November 2025

Copyright : Author
Publish by : CAUSA

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

tersebut menimbulkan risiko signifikan terhadap hak asasi manusia, terutama hak atas privasi dan kebebasan berekspresi. Penelitian ini bertujuan untuk menganalisis bentuk dan batas kewenangan negara dalam pengawasan ruang digital berdasarkan kerangka hukum nasional serta merumuskan mekanisme akuntabilitas yang ideal agar pengawasan tidak berubah menjadi tindakan represif. Dengan menggunakan pendekatan yuridis normatif dan analisis kualitatif terhadap peraturan perundang-undangan, putusan Mahkamah Konstitusi, serta literatur akademik, penelitian ini menemukan bahwa kewenangan pengawasan negara harus tunduk pada prinsip legalitas, tujuan yang sah, kebutuhan, dan proporsionalitas. Penelitian ini juga menegaskan perlunya penguatan mekanisme pengawasan melalui otorisasi yudisial independen, transparansi publik, pengawasan multi-lapis, serta peran otoritas pelindungan data pribadi yang benar-benar independen. Hasil penelitian menunjukkan bahwa penyusunan regulasi pengawasan digital yang komprehensif dan berbasis HAM menjadi kebutuhan mendesak untuk menjaga keseimbangan antara kepentingan publik dan perlindungan hak asasi manusia di Indonesia.

Kata kunci: pengawasan digital, hak asasi manusia, privasi, negara hukum, akuntabilitas.

PENDAHULUAN

Ruang digital saat ini telah menjadi arena utama bagi kehidupan sosial, politik, ekonomi, dan budaya masyarakat modern sehingga pengawasan dan regulasi atas ruang tersebut memberi dampak langsung pada kualitas demokrasi dan penikmatan hak asasi.[1] Selama dekade terakhir, perkembangan teknologi pengumpulan data dan kecerdasan buatan (AI) meningkatkan kapasitas negara untuk melakukan pengawasan massal yang lebih cepat, lebih luas, dan lebih terpersonalisasi praktik yang membawa manfaat keamanan sekaligus menimbulkan risiko serius terhadap privasi dan kebebasan berekspresi.[2] Selain itu, Termasuk dalam tantangan tersebut adalah bagaimana negara menggunakan pengawasan sering atas nama kepentingan publik seperti keamanan nasional, ketertiban umum atau perlindungan pemilu namun dapat menjadi sarana pembatasan kebebasan berekspresi jika tidak dibarengi mekanisme akuntabilitas dan perlindungan HAM yang memadai. Misalnya, organisasi internasional telah mengingatkan bahwa *"any use of digital surveillance technologies … must be fully human rights compliant."*.[3]

[1] Masferrer, Aniceto. *The Decline of Freedom of Expression and Social Vulnerability in Western democracy.* Int J Semiot Law. 2023. doi: 10.1007/s11196-023-09990-1.

[2] Azgin, Bilge & Kiralp, Sevki. *"Surveillance, Disinformation, and Legislative Measures in the 21st Century: AI, Social Media, and the Future of Democracies." Social Sciences* 13 (2024): 510.

[3] https://www.icj.org/covid-19-use-of-digital-surveillance-technologies-must-be-human-rights-compliant/?utm_source=chatgpt.com diakses pada 13 November 2025

Secara praktis, berbagai permasalahan muncul: (a) kerangka hukum pengawasan elektronik yang seringkali belum memenuhi prinsip legalitas, proporsionalitas, dan transparansi;[4] (b) minimnya mekanisme pengawasan independen terhadap praktik pengumpulan dan pemrosesan data oleh aparat negara;[5] dan (c) keterlibatan perusahaan platform digital yang berada di antara kewajiban untuk menghormati HAM dan tekanan negara untuk memberikan akses data atau menurunkan konten sehingga muncul fenomena "privatisasi sensor" yang memunculkan ketidakjelasan tanggung jawab hukum.[6] Di negara berkembang seperti Indonesia, tantangan makin kompleks karena adanya kebutuhan untuk menyeimbangkan pembangunan digital dan keamanan dengan perlindungan hak-hak sipil, sementara kapasitas regulasi dan pengawasan masih terbatas.[7]

Penelitian ini menjadi sangat relevan karena: pertama, masih terdapat kekosongan dalam literatur empiris dan konseptual terkait bagaimana keseimbangan antara kepentingan publik (sekuriti, ketertiban, keutuhan informasi publik) dan HAM (privasi, kebebasan berekspresi) implementatif dalam praktik pengawasan digital.[8] Kedua, regulasi digital yang semakin baru misalnya undang-undang perlindungan data, regulasi *platform,* aturan keamanan siber memerlukan evaluasi hukum yang menilai kesesuaian dengan standar HAM internasional, terutama prinsip proporsionalitas, akses pengadilan, dan pengawas independen.[9] Ketiga, terdapat bukti bahwa intervensi negara di ruang digital dapat berdampak pada partisipasi publik, kualitas informasi publik, dan legitimasi proses demokrasi membuat kajian ini penting untuk merumuskan rekomendasi kebijakan yang seimbang dan berbasis HAM.[10]

Oleh karena itu, penelitian ini penting dilakukan karena memberikan analisis hukum normatif dan komparatif terkait batas-batas sah pengawasan negara di ruang digital agar kebijakan publik tidak melanggar hak asasi manusia (HAM).[11] Penelitian ini juga mengisi kekosongan literatur mengenai bagaimana prinsip-prinsip HAM diterjemahkan dalam praktik pengawasan digital di negara-negara dengan kondisi politik dan regulasi yang berbeda.[12] Selain itu, penelitian ini menghasilkan rekomendasi kebijakan yang dapat membantu pembuat kebijakan, badan pengawas, dan masyarakat sipil dalam menegakkan akuntabilitas serta perlindungan HAM di era digital tanpa mengorbankan kepentingan publik yang sah.[13]

Rumusan masalah:

1. Bagaimana bentuk dan batas kewenangan negara dalam melakukan pengawasan terhadap ruang digital menurut perspektif hukum nasional tentang hak asasi manusia?

---

[4] *Ibid*

[5] Tsung-Ling Lee, Sharifah Sekalala & Pedro Villarreal, *"AI and Data Surveillance: Embedding a Human Rights-based Approach,"* Journal of Law, Medicine & Ethics, online 14 April 2025.

[6] *Ibid*

[7] Manan Laila, Sajjad & Dr Muhammad Zakir, *"Digital Surveillance, Migration Control, and Human Rights: Ethical Dilemmas in the Use of Technology to Govern Human Mobility,"* Inverge Journal of Social Sciences 4(3) (2024): –; DOI:10.63544/ijss.v4i3.170.

[8] Khan Wajahat & S. Naseeb, *"Digital Rights and Data Privacy in the Age of Surveillance: A Comparative Analysis of International Standards,"* Mayo Communication Journal 1(1) (2024): 22-30.

[9] *Ibid*

[10] Praveen S. Chauhan & Prashant K. Gangwar, *"Digital human rights: Jurisprudential perspective of cybersecurity and data protection,"* International Journal of Civil Law and Legal Research 5(1) (2025): 18-31.

[11] *Ibid*

[12] Chaerul Shaleh et al., *"Human Rights in the Control of Digital Public Space Freedom: A Collaborative Approach Based on Islamic Law Principles,"* Jurnal Hukum Islam 23(1) (2024): –; DOI:10.28918/jhi.v23i1.01.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

2. Bagaimana mekanisme akuntabilitas dan pengawasan hukum yang ideal untuk menyeimbangkan antara kepentingan publik dan perlindungan hak asasi manusia dalam praktik pengawasan digital di Indonesia?

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif dengan metode analisis kualitatif-deskriptif. Pendekatan ini berfokus pada kajian terhadap norma hukum yang mengatur pengawasan negara atas ruang digital serta perlindungan hak asasi manusia (HAM). Sebagaimana dijelaskan oleh Marzuki, penelitian hukum normatif dilakukan "dengan meneliti bahan pustaka atau data sekunder melalui kajian terhadap teori, konsep, dan peraturan perundang-undangan yang relevan."[13]

Jenis penelitian ini adalah hukum normatif yang membahas tentang Antara Kepentingan Publik Dan Hak Asasi: Analisis Hukum Terhadap Pengawasan Negara Atas Ruang Digital. Pendekatan yang digunakan dalam penelitian ini adalah menggunakan pendekatan undang-undang dan menelusuri literatur-literatur yang berkaitan dengan objek penelitian, istilah pendekatan dengan metode pendekatan undang-undang dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkutan dengan isu hukum yang sedang ditangani.[14] Penelitian yang dilakukan bersifat deskriptif yaitu menggambarkan gejala-gejala di lingkungan masyarakat terhadap suatu kasus yang diteliti, pendekatan yang dilakukan yaitu pendekatan kualitatif yang merupakan tata cara penelitian yang menghasilkan data deskriptif. Digunakan pendekatan kualitatif oleh penulis bertujuan untuk mengerti atau memahami gejala yang diteliti. Penulis melakukan penelitian dengan tujuan mencari taraf sinkronisasi hukum yang terjadi pada masyarakat antara hukum positif dengan apa yang terjadi di tengah tengah masyarakat.

Cara pengumpulan data dalam penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan-bahan hukum, baik bahan hukum primer, bahan hukum sekunder, maupun bahan hukum tersier yang digunakan adalah penelusuran penelusuran di internet dan keaktifan penulis untuk membaca literatur-literatur kepustakaan yang mewakili korelasi tentang Antara Kepentingan Publik Dan Hak Asasi: Analisis Hukum Terhadap Pengawasan Negara Atas Ruang Digital.

PEMBAHASAN

A. Bentuk dan Batas Kewenangan Negara dalam Melakukan Pengawasan Terhadap Ruang Digital Menurut Perspektif Hukum Nasional Tentang Hak Asasi Manusia

Perkembangan teknologi informasi dan komunikasi telah melahirkan ruang baru yang lazim disebut sebagai ruang digital, yang melebur batas antara ranah privat dan publik. Dalam perspektif negara hukum demokratis, ruang digital tidak berdiri terpisah dari tatanan hukum yang sudah ada, melainkan merupakan perluasan dari ruang kehidupan warga negara yang hak-hak konstitusionalnya tetap melekat dan wajib dilindungi. UUD NRI 1945 melalui Bab XA secara

[13] Marzuki, Peter Mahmud. (2016). *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana. Hlm 50-55
[14] Amiruddin dan H Zainal Asikin. Pengantar Metode Penelitian Hukum. Jakarta: Raja Grafindo Persada, 2006, halaman 118.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

tegas mengakui dan menjamin hak-hak asasi manusia, termasuk hak untuk berkomunikasi, memperoleh dan menyebarkan informasi, hak atas rasa aman, serta hak atas perlindungan diri pribadi sebagaimana tercermin antara lain dalam Pasal 28E dan Pasal 28G ayat (1). Hak-hak tersebut kemudian dikonkritkan lebih lanjut dalam Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia yang memberikan pengaturan eksplisit mengenai hak atas privasi, kerahasiaan korespondensi, dan kebebasan berekspresi. Dalam kerangka ini, setiap bentuk pengawasan negara terhadap aktivitas warga di ruang digital harus dipandang sebagai tindakan yang secara potensial menyentuh domain hak asasi, sehingga tidak dapat dilepaskan dari prinsip-prinsip dasar hukum HAM[15].

Kewenangan negara untuk melakukan pengawasan di ruang digital lahir dari kewajiban negara untuk menghormati, melindungi, dan memenuhi hak asasi manusia. Kewajiban melindungi *(to protect)* mendorong negara membangun sistem yang mampu mencegah dan menanggulangi kejahatan siber, ancaman terhadap keamanan nasional, disinformasi yang membahayakan ketertiban umum, hingga serangan terhadap infrastruktur kritis. Namun di sisi lain, kewajiban menghormati *(to respect)* dan memenuhi *(to fulfil)* hak asasi mengharuskan negara menahan diri agar upaya pengawasan tidak berkembang menjadi praktik yang represif, invasif, atau bahkan menjadi bentuk pembatasan hak yang sewenang-wenang. Literatur hukum siber dan hak asasi manusia di Indonesia menegaskan bahwa hak atas privasi termasuk privasi informasi dan data pribadi merupakan hak konstitusional yang mendapatkan penguatan yuridis di era digital, sehingga pengawasan negara terhadap komunikasi dan data warga harus dibaca sebagai bentuk pembatasan hak yang hanya dapat dibenarkan dalam kondisi tertentu dan dengan prosedur yang ketat[16].

Secara normatif, bentuk kewenangan pengawasan negara terhadap ruang digital tersebar dalam sejumlah peraturan perundang-undangan. Undang-Undang tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya memberikan dasar hukum bagi intersepsi atau penyadapan terhadap informasi dan/atau dokumen elektronik untuk kepentingan penegakan hukum, serta bagi pemutusan akses terhadap konten yang dianggap melanggar hukum. UU ITE juga mengatur kewajiban penyelenggara sistem elektronik untuk menyimpan dan menyediakan data elektronik tertentu kepada aparat penegak hukum. Di sisi lain, Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memberikan kewenangan kepada Badan Intelijen Negara untuk mengumpulkan, mengolah, dan menganalisis informasi, termasuk melalui instrumen teknologi informasi, dalam rangka menjaga keamanan nasional. Kewenangan tersebut diperkuat oleh sejumlah ketentuan sektoral lain yang memberikan dasar bagi pengawasan lalu lintas komunikasi dan data, misalnya di bidang telekomunikasi, perbankan, dan perpajakan

Perkembangan penting dalam lanskap pengawasan digital di Indonesia adalah hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini memposisikan perlindungan data pribadi sebagai bagian dari upaya menjamin hak konstitusional subjek data, yaitu hak atas privasi dan perlindungan diri pribadi sebagaimana dimaksud dalam Pasal 28G ayat (1) UUD 1945. UU PDP bukan hanya mengatur kewajiban pengendali dan prosesor data pribadi di sektor privat, tetapi juga mengikat lembaga negara yang memproses data warga

[15] Nanik Qurrotuaini, "Hak Privasi sebagai Hak Konstitusional di Era Digital," *Staatsrecht: Indonesian Constitutional Law Journal* 5, no. 1 (2024).
[16] Komang Ratih Anggen Suari, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi sebagai Hak Asasi Manusia," *Jurnal Ilmiah Akuntansi dan Humanika* 13, no. 1 (2023).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

dalam konteks pelayanan publik, penegakan hukum, maupun intelijen.[17] Dalam tataran tertentu, UU PDP menempatkan negara bukan sekadar pemegang otoritas pengawasan, tetapi juga sebagai subjek yang harus tunduk pada standar akuntabilitas dan prinsip kehati-hatian *(due care)* dalam memproses data warga, termasuk ketika pengumpulan dan pemrosesan data tersebut dilakukan atas nama pengawasan keamanan dan penegakan hukum.

Meskipun berbagai undang-undang memberikan legitimasi terhadap adanya pengawasan digital, batas kewenangan negara sepenuhnya ditentukan oleh standar hak asasi manusia. Hak atas privasi, kebebasan berkomunikasi, dan kebebasan berekspresi menjadi "batas pagar" normatif yang tidak boleh dilampaui. Penelitian Qurrotuaini tentang hak privasi sebagai hak konstitusional di era digital menegaskan bahwa setiap bentuk intervensi negara terhadap arus data dan komunikasi warga harus dipandang sebagai pengecualian dari keadaan normal, sehingga memerlukan pembuktian yang ketat atas dasar pembenarannya. Mahkamah Konstitusi dalam berbagai putusan terkait penyadapan menyatakan bahwa tindakan penyadapan merupakan bentuk pembatasan hak atas privasi yang bersifat serius, sehingga hanya dapat dibenarkan jika diatur secara eksplisit dalam undang-undang, dilakukan untuk tujuan yang sah, dan disertai dengan mekanisme kontrol yang efektif.

Dari perspektif HAM, batas kewenangan pengawasan negara umumnya dirumuskan ke dalam empat prinsip utama, yaitu legalitas, tujuan yang sah *(legitimate aim)*, kebutuhan *(necessity)*, dan proporsionalitas *(proportionality)*. Prinsip legalitas mengharuskan bahwa tindakan pengawasan hanya dapat dilakukan jika diatur secara jelas, rinci, dan dapat diprediksi dalam undang-undang, bukan semata-mata berdasarkan kebijakan administratif atau peraturan turunan yang sifatnya teknis. Prinsip tujuan yang sah menuntut bahwa intervensi hanya boleh dilakukan untuk melindungi kepentingan yang diakui oleh konstitusi dan hukum HAM, seperti keamanan nasional, ketertiban umum, atau perlindungan hak orang lain, bukan untuk mengamankan kepentingan politik kekuasaan atau meredam kritik. Prinsip kebutuhan mengharuskan bahwa pengawasan hanya ditempuh jika tidak ada alternatif lain yang lebih lunak dan kurang intrusif. Sementara itu, prinsip proporsionalitas menuntut adanya keseimbangan antara intensitas pengawasan dan tingkat ancaman yang hendak diatasi, termasuk pembatasan ruang lingkup, durasi, dan jenis data yang diakses[18].

Dalam praktik, prinsip-prinsip tersebut semakin relevan ketika pengawasan dilakukan dengan memanfaatkan teknologi yang sangat intrusif, seperti penyadapan *real-time*, pemantauan media sosial secara masif, pengumpulan metadata dalam jumlah besar, dan penggunaan kecerdasan artifisial untuk *profiling*. Sejumlah kajian, termasuk laporan lembaga seperti ELSAM, ICJR, dan SAFEnet, menunjukkan adanya kecenderungan perluasan kewenangan pengawasan negara, baik melalui kerja sama dengan operator telekomunikasi maupun melalui pemanfaatan platform digital, yang menimbulkan kekhawatiran atas potensi praktik pengawasan massal yang tidak sepenuhnya transparan. Kekhawatiran ini beralasan karena pengawasan yang dilakukan tanpa batas, tanpa otorisasi yudisial yang memadai, dan tanpa mekanisme pertanggungjawaban yang jelas akan berpotensi melanggar hak atas privasi dan

[17] Aisya Shafira Sumarahati, "Analisis Yuridis Perlindungan Hak Asasi Manusia dalam Penegakan Hukum Elektronik," *Indonesian Journal of Islamic Law and Justice* 6, no. 2 (2024).
[18] Dimas Endri Mahameruaji et al., "Implementasi UU Pelindungan Data Pribadi untuk Keamanan Identitas di Indonesia," *Jurnal Esensi Hukum* 5, no. 1 (2023).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

kebebasan berekspresi, serta menciptakan *chilling effect* terhadap partisipasi warga di ruang digital.

Dengan demikian, secara konseptual dapat disimpulkan bahwa bentuk kewenangan negara dalam pengawasan ruang digital di Indonesia meliputi intersepsi komunikasi elektronik, pengumpulan dan analisis data, pemantauan lalu lintas informasi, serta pemutusan akses terhadap konten digital berdasarkan peraturan perundang-undangan yang berlaku. Namun, kewenangan ini tidak bersifat absolut. Perspektif hukum nasional tentang hak asasi manusia menempatkan kewenangan tersebut dalam batas-batas konstitusional yang ketat melalui jaminan hak atas privasi, kebebasan berekspresi, kerahasiaan korespondensi, serta perlindungan data pribadi. Pembatasan hanya dapat dilakukan sejauh memenuhi syarat legalitas, tujuan sah, kebutuhan, dan proporsionalitas, serta didukung mekanisme pengawasan dan akuntabilitas yang efektif. Di luar kerangka itu, pengawasan negara terhadap ruang digital berisiko bergeser menjadi praktik yang bertentangan dengan prinsip negara hukum dan hak asasi manusia.

B. Mekanisme Akuntabilitas dan Pengawasan Hukum yang Ideal untuk Menyeimbangkan Antara Kepentingan Publik dan Perlindungan Hak Asasi Manusia dalam Praktik Pengawasan Digital di Indonesia

Isu utama dalam praktik pengawasan digital di Indonesia bukan semata-mata ada atau tidaknya kewenangan negara untuk melakukan pengawasan, melainkan bagaimana kewenangan tersebut dipertanggungjawabkan sehingga tidak berujung pada pelanggaran hak asasi manusia. Dalam beberapa tahun terakhir, berbagai laporan lembaga nasional dan internasional mengenai situasi hak-hak digital di Indonesia menggarisbawahi problem lemahnya akuntabilitas dalam praktik pengawasan, baik yang dilakukan atas nama penegakan hukum, keamanan siber, maupun tata kelola data oleh lembaga publik. Laporan *Freedom on the Net*, laporan situasi hak-hak digital SAFEnet, serta kajian ELSAM dan ICJR menunjukkan potret yang relatif konsisten: di satu sisi, negara terus memperluas instrumen regulatif di ruang siber; di sisi lain, mekanisme kontrol terhadap penggunaan instrumen tersebut masih parsial, tidak transparan, dan belum sepenuhnya berorientasi pada HAM.

Secara normatif, kerangka akuntabilitas pengawasan digital di Indonesia sebenarnya sudah memiliki sejumlah "pilar", antara lain mekanisme pengujian undang-undang oleh Mahkamah Konstitusi, kewajiban perintah hakim dalam pembatasan hak tertentu, keberadaan Komnas HAM dan lembaga pengawas sektoral, serta fungsi pengawasan DPR terhadap kebijakan pemerintah. Mahkamah Konstitusi, misalnya, melalui berbagai putusannya menegaskan bahwa tindakan penyadapan dan pembatasan hak privasi harus ditempatkan sebagai bentuk pembatasan HAM yang hanya dapat dilakukan berdasarkan undang-undang dan dengan mekanisme pengawasan yang memadai. Putusan-putusan tersebut tidak hanya menilai konstitusionalitas norma, tetapi sekaligus memberikan pedoman bahwa legislator dan penegak hukum wajib menjamin adanya kontrol independen atas praktik pengawasan[19].

Di luar itu, Undang-Undang Perlindungan Data Pribadi menghadirkan dimensi akuntabilitas baru dengan mewajibkan keberadaan otoritas pengawas data pribadi yang bersifat independen. Otoritas ini dirancang untuk menerima pengaduan, melakukan pemeriksaan, dan

[19] Muhammad Alim, "Konstitusionalitas Penyadapan dalam Perspektif Hak Asasi Manusia," *Jurnal Konstitusi* 17, no. 3 (2020).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

menjatuhkan sanksi administratif atas pelanggaran perlindungan data, termasuk oleh lembaga negara. Dari perspektif hak asasi manusia, kehadiran otoritas pengawas ini penting karena untuk pertama kalinya terdapat lembaga spesifik yang berfungsi sebagai "penyeimbang" ketika negara atau korporasi memproses data pribadi warga dalam skala besar. Namun, berbagai analisis mutakhir menunjukkan bahwa efektivitas otoritas ini sangat bergantung pada desain kelembagaannya, jaminan independensi, kecukupan kewenangan, dan dukungan politik maupun anggaran[20].

Walaupun demikian, kerangka yang ada masih menyisakan sejumlah kelemahan mendasar. Pertama, pengaturan mengenai pengawasan digital tersebar di berbagai undang-undang sektoral tanpa adanya satu undang-undang induk yang komprehensif mengenai pengawasan dan penyadapan. Fragmentasi ini menyebabkan standar prosedural, syarat otorisasi, jenis data yang boleh diakses, dan jangka waktu pengawasan berbeda-beda antar sektor, sehingga membuka ruang interpretasi luas dan berpotensi menciptakan celah penyalahgunaan kewenangan.

Kedua, di sejumlah rezim pengawasan, otorisasi yudisial yang idealnya menjadi mekanisme kontrol independen justru tidak selalu diatur secara eksplisit. Penyadapan atau akses data terkadang cukup didasarkan pada persetujuan pejabat internal atau kesepakatan administratif dengan operator telekomunikasi, yang jelas lebih rentan terhadap konflik kepentingan dan kurang memenuhi standar *impartiality* sebagaimana dituntut oleh prinsip HAM.

Ketiga, tingkat transparansi atas praktik pengawasan digital masih sangat terbatas. Tidak terdapat kewajiban yang tegas bagi lembaga penegak hukum ataupun lembaga intelijen untuk menerbitkan laporan transparansi tahunan yang berisi jumlah permintaan data, jumlah penyadapan yang dilakukan, dasar hukum yang digunakan, dan hasil atau tingkat keberhasilannya. Padahal, di banyak negara, laporan seperti ini menjadi salah satu instrumen penting dalam mencegah penyalahgunaan kewenangan pengawasan. Keterbatasan transparansi tersebut berdampak pada sulitnya masyarakat sipil, akademisi, maupun lembaga pengawas eksternal melakukan pengujian publik *(public scrutiny)* terhadap praktik pengawasan.

Keempat, mekanisme pemulihan *(remedies)* bagi warga yang menjadi korban pengawasan sewenang-wenang masih belum terbangun secara jelas. Walaupun tersedia saluran pengaduan ke Komnas HAM, Ombudsman, atau gugatan perdata dan pidana, realitas menunjukkan bahwa hambatan pengetahuan, biaya, dan kompleksitas prosedur masih cukup besar. Literatur mengenai hak atas privasi dan data pribadi di Indonesia menunjukkan bahwa banyak kasus pelanggaran privasi tidak berujung pada pemulihan yang memadai, baik karena tidak adanya informasi bahwa seseorang telah diawasi, maupun karena ketiadaan jalur prosedural yang sederhana dan efektif bagi korban.

Berangkat dari kondisi tersebut, sejumlah akademisi dan organisasi masyarakat sipil mengusulkan desain mekanisme akuntabilitas yang lebih ideal. Salah satu usulan kunci adalah pembentukan undang-undang khusus mengenai pengawasan dan penyadapan yang mengintegrasikan seluruh bentuk pengawasan komunikasi dan data di berbagai sektor. Undang-undang ini diharapkan mengatur secara komprehensif definisi tindakan pengawasan, lembaga yang berwenang, standar pembenaran, prosedur permohonan dan pemberian izin, batas durasi

[20] A. Zulfikar Nurkamal, "Perlindungan Hukum Korban Pelanggaran Hak Atas Privasi di Era Digital," *Indonesian Journal of Criminal Law and Criminology* 3, no. 2 (2024).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

dan cakupan pengawasan, serta mekanisme evaluasi dan penghentian tindakan pengawasan. Dengan demikian, tidak ada lagi ruang abu-abu di mana lembaga tertentu melakukan pengawasan dengan dasar hukum yang tidak jelas atau bertumpu hanya pada regulasi turunan[21].

Selain penguatan pada tataran normatif, mekanisme akuntabilitas ideal mewajibkan adanya otorisasi yudisial independen untuk setiap tindakan pengawasan yang bersifat intrusif, terutama penyadapan dan penggeledahan digital. Hakim atau pengadilan khusus harus menjadi otoritas yang menilai apakah syarat-syarat legalitas, tujuan sah, kebutuhan, dan proporsionalitas telah terpenuhi sebelum memberi izin. Desain seperti ini sejalan dengan doktrin konstitusional tentang perlindungan data pribadi sebagai bagian dari perlindungan diri pribadi yang dijamin Pasal 28G ayat (1) UUD 1945 dan ditegaskan kembali oleh Mahkamah Konstitusi. Penguatan judicial oversight juga menjadi penyangga penting agar cabang kekuasaan eksekutif tidak memonopoli penentuan kapan dan terhadap siapa pengawasan dapat dilakukan.

Mekanisme akuntabilitas yang ideal juga menuntut penguatan otoritas pengawas data pribadi sebagai lembaga yang benar-benar independen, baik secara struktural, fungsional, maupun anggaran. Otoritas ini perlu memiliki kewenangan untuk mengaudit praktik pengawasan yang melibatkan pemrosesan data pribadi, termasuk yang dilakukan oleh lembaga penegak hukum dan intelijen, serta menjatuhkan sanksi ketika ditemukan pelanggaran. Di samping itu, pengawasan terhadap pengawasan *(oversight of surveillance)* perlu dilakukan secara berlapis, yaitu oleh pengadilan, lembaga pengawas internal, lembaga HAM, dan lembaga legislatif. Pendekatan multi-lapis seperti ini memungkinkan setiap tindakan pengawasan diuji dari berbagai sudut: kepatuhan terhadap hukum prosedural, kesesuaian dengan standar HAM, serta pertanggungjawaban politik dan kebijakan.

Transparansi dan partisipasi publik merupakan elemen lain yang tidak terpisahkan dari mekanisme akuntabilitas yang ideal. Lembaga negara yang memiliki kewenangan pengawasan digital perlu diwajibkan secara hukum menerbitkan laporan transparansi yang dapat diakses publik, memuat data agregat mengenai permintaan data, tindakan penyadapan, pemblokiran konten, dan dasar hukum yang digunakan. Pada saat yang sama, proses penyusunan dan evaluasi regulasi pengawasan digital harus membuka ruang konsultasi yang memadai dengan akademisi, organisasi masyarakat sipil, komunitas teknologi, dan masyarakat umum. Dengan demikian, regulasi yang lahir tidak hanya merefleksikan perspektif keamanan dan penegakan hukum, tetapi juga sensitif terhadap perlindungan hak asasi manusia dan kebebasan sipil.

Mekanisme akuntabilitas yang baik juga wajib memberikan perlindungan khusus bagi kelompok rentan dan aktor demokrasi kunci seperti jurnalis, pembela hak asasi manusia, dan oposisi politik. Sejumlah riset terbaru menunjukkan bahwa kelompok-kelompok ini lebih rentan menjadi target pengawasan, baik melalui instrumen hukum maupun serangan digital, sehingga berpotensi menimbulkan dampak pembungkaman *(chilling effect)* terhadap kebebasan berekspresi dan ruang sipil. Oleh karena itu, standar pembenaran pengawasan terhadap mereka harus lebih ketat, misalnya mensyaratkan pengawasan hanya dapat dilakukan jika terkait dengan dugaan kejahatan serius dan memperoleh izin dari pengadilan tingkat lebih tinggi[22].

[21] Wahyudi Djafar, "The Urgency of Human Rights-Based Digital Governance in Indonesia," *Journal of Southeast Asian Human Rights* (2022).
[22] Freedom House, "Freedom on the Net Report: Indonesia," *Freedom House Journal* (2023).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Akhirnya, mekanisme akuntabilitas dan pengawasan hukum yang ideal harus bersifat adaptif dan responsif terhadap dinamika teknologi. Reformasi hukum di ruang siber tidak dapat bersifat sekali jadi, melainkan perlu dirancang dengan klausul evaluasi berkala dan penyesuaian regulasi terhadap perkembangan seperti kecerdasan artifisial, *big data analytics,* dan *Internet of Things*. Penelitian mutakhir mengenai perlindungan HAM di era digital menegaskan bahwa perkembangan teknologi cenderung melampaui kecepatan pembaruan hukum, sehingga diperlukan desain regulasi yang fleksibel namun berprinsip, dengan menjadikan standar HAM sebagai titik acuan utama dalam setiap pembaruan.

Berdasarkan uraian tersebut dapat ditegaskan bahwa mekanisme akuntabilitas dan pengawasan hukum yang ideal dalam praktik pengawasan digital di Indonesia adalah mekanisme yang menggabungkan kerangka normatif yang komprehensif, otorisasi yudisial independen, pengawasan multi-lapis, transparansi dan partisipasi publik, perlindungan khusus bagi kelompok rentan, serta sifat adaptif terhadap perkembangan teknologi. Hanya dengan desain seperti ini keseimbangan antara kepentingan publik dalam bentuk keamanan, ketertiban, dan penegakan hukum dan perlindungan hak asasi manusia di ruang digital dapat diwujudkan secara konsisten dalam praktik.

KESIMPULAN

Penelitian ini menyimpulkan bahwa pengawasan negara atas ruang digital merupakan kewenangan yang sah sepanjang dilakukan untuk melindungi kepentingan publik seperti keamanan nasional, ketertiban umum, dan penegakan hukum. Namun, kewenangan tersebut tidak bersifat tanpa batas. Berdasarkan UUD 1945, UU HAM, UU ITE, dan UU PDP, setiap bentuk pengawasan yang menyentuh privasi, komunikasi, atau data pribadi warga negara harus tunduk pada prinsip legalitas, tujuan yang sah, kebutuhan, dan proporsionalitas. Dengan demikian, pengawasan negara hanya dapat dibenarkan apabila memiliki dasar hukum yang jelas, dilakukan untuk kepentingan yang benar-benar sah, dan merupakan langkah terakhir yang paling diperlukan serta tidak berlebihan.

Di sisi lain, praktik pengawasan digital di Indonesia masih menghadapi persoalan akuntabilitas, antara lain minimnya otorisasi yudisial yang independen, rendahnya transparansi, lemahnya mekanisme pengawasan eksternal, serta belum adanya regulasi khusus yang mengatur pengawasan dan penyadapan secara komprehensif. Oleh karena itu, mekanisme akuntabilitas yang ideal harus dibangun melalui penguatan peran pengadilan, otoritas perlindungan data pribadi yang independen, pengawasan multi-lapis, kewajiban laporan transparansi, serta perlindungan khusus bagi kelompok rentan seperti jurnalis dan pembela HAM. Dengan mekanisme tersebut, keseimbangan antara kepentingan publik dan perlindungan hak asasi manusia di ruang digital dapat diwujudkan secara lebih konkret dan konsisten.

DAFTAR PUSTAKA

Alim, Muhammad. *"Konstitusionalitas Penyadapan dalam Perspektif Hak Asasi Manusia." Jurnal Konstitusi* 17, No. 3 (2020).

Amiruddin, A. Z. (2006). *Pengantar Metode Penelitian Hukum Jakarta*: Raja Grafindo

Anggen Suari, Komang Ratih. *"Menjaga Privasi di Era Digital: Perlindungan Data Pribadi sebagai Hak Asasi Manusia."* Jurnal Ilmiah Akuntansi dan Humanika 13, No. 1 (2023).

Azgin, B., & Kiralp, S. (2024). *Surveillance, Disinformation, and Legislative Measures in the 21st Century: AI, Social Media, and the Future of Democracies. Social Sciences*, *13*(10), 510. DOI: https://doi.org/10.3390/socsci13100510

Digital Rights and Data Privacy in the Age of Surveillance A Comparative Analysis of International Standards. (2024). Mayo Communication Journal , 1(1), 22-30. https://researchcorridor.org/index.php/mcj/article/view/144

Global Freedom House. "Freedom on the Net Report: Indonesia." Freedom House Journal (2023).

International Commission of Jurists, "COVID-19: Use of digital surveillance technologies must be human rights compliant," 2 April 2020.

Lee, T.-L., Sekalala, S., & Villarreal, P. (2025). *AI and Data Surveillance: Embedding a Human Rights-based Approach. Journal of Law, Medicine & Ethics*, *53*(S1), 70–74. DOI: 10.1017/jme.2025.17.

Mahameruaji, Dimas Endri, dkk. *"Implementasi UU Pelindungan Data Pribadi untuk Keamanan Identitas di Indonesia."* Jurnal Esensi Hukum 5, No. 1 (2023).

Manan, L., Sajjad, & Zakir, M. (2024). *Digital surveillance, migration control, and human rights: Ethical dilemmas in the use of technology to govern human mobility. Inverge Journal of Social Sciences, 4*(3). DOI: https://doi.org/10.63544/ijss.v4i3.170

Marzuki, M. (2017). *Penelitian hukum: Edisi revisi*. Prenada Media.

Masferrer A. (2023). *The Decline of Freedom of Expression and Social Vulnerability in Western democracy. International journal for the semiotics of law = Revue internationale de semiotique juridique, 1-33. Advance online publication.* DOI: https://doi.org/10.1007/s11196-023-09990-1

Nurkamal, A. Zulfikar. *"Perlindungan Hukum Korban Pelanggaran Hak Atas Privasi di Era Digital." Indonesian Journal of Criminal Law and Criminology* 3, No. 2 (2024).

Qurrotuaini, Nanik. *"Hak Privasi sebagai Hak Konstitusional di Era Digital." Staatsrecht: Indonesian Constitutional Law Journal* 5, No. 1 (2024)

Shaleh, C., Rasyid, F. A., Sonjaya, A., & Abdulrahman, M. M. (2025). *Human Rights in the Control of Digital Public Space Freedom: A Collaborative Approach Based on Islamic Law Principles. Jurnal Hukum Islam*, *23*(1), 1–36. DOI: https://doi.org/10.28918/jhi.v23i1.01

Sumarahati, Aisya Shafira. *"Analisis Yuridis Perlindungan Hak Asasi Manusia dalam Penegakan Hukum Elektronik." Indonesian Journal of Islamic Law and Justice* 6, No. 2 (2024).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 1 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Wahyudi, Djafar. "*The Urgency of Human Rights-Based Digital Governance in Indonesia.*" *Journal of Southeast Asian Human Rights* (2022).