

## Balancing National Security and Civil Liberties: Human Rights Implications of Digital Surveillance Policies in Southeast Asia

Methodius Kossay\*<sup>1</sup>, Maulana Fahmi Idris<sup>2</sup>

<sup>1,2</sup>Program Studi Ilmu Hukum, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia

E-mail: [methodius@stekom.ac.id](mailto:methodius@stekom.ac.id)

| Article Info                                                                                                                    | Abstract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keywords:</b><br>Digital surveillance,<br>Human rights,<br>National security,<br>Civil liberties,<br>Comparative Legal Study | <i>The rapid expansion of digital surveillance technologies has intensified debates regarding the balance between national security and civil liberties. In Southeast Asia, governments increasingly employ digital surveillance to address cybersecurity threats, terrorism, online extremism, and transnational crime. However, the expansion of surveillance powers raises concerns regarding privacy rights, freedom of expression, and broader human rights protections. Despite growing scholarly attention, limited studies have comparatively examined how ASEAN member states reconcile security imperatives with human rights obligations within a regional framework characterized by both human rights commitments and strong sovereignty principles. This study investigates the human rights implications of digital surveillance policies in Southeast Asia through a comparative regional legal analysis of six ASEAN member states: Indonesia, Singapore, Malaysia, Thailand, Vietnam, and the Philippines. Using a qualitative doctrinal-comparative approach, the study analyzes constitutions, cybersecurity laws, data protection regulations, surveillance-related legislation, and relevant policy documents. The analysis is guided by Securitization Theory and Human Rights Governance. The findings indicate that all examined states have institutionalized digital surveillance as a component of national security governance, although significant differences exist in legal safeguards, oversight mechanisms, transparency, and rights protections. The study demonstrates that variations in surveillance governance are shaped by the interaction between the degree of threat securitization and the strength of domestic human rights institutions. Based on these findings, the study develops the ASEAN Surveillance Governance Typology, consisting of Security-Dominant, Security-Oriented Hybrid, Hybrid, and Rights-Constrained models.</i> |

**DOI:** <https://doi.org/10.51903/8zwvcq64>

Submitted: April 2026, Reviewed: May 2026, Accepted: June 2026

Corresponding Author

### I. PENDAHULUAN

Perkembangan teknologi pengawasan digital telah menjadi salah satu transformasi tata kelola yang paling signifikan pada abad ke-21. Kemajuan pesat dalam kecerdasan buatan (*artificial intelligence*), sistem identifikasi biometrik, teknologi pengenalan wajah (*facial recognition*), analisis data besar (*big data analytics*), dan pemrosesan data secara *real-time* telah meningkatkan kapasitas negara dalam memantau, mengklasifikasikan, serta mengendalikan berbagai aktivitas sosial masyarakat (Broeders et al., 2023; Matey, 2024). Pemerintah di berbagai belahan dunia semakin mengandalkan teknologi tersebut untuk menghadapi beragam ancaman keamanan, mulai dari terorisme, kejahatan siber,

ekstremisme digital, penyebaran disinformasi, hingga kejahatan transnasional yang memanfaatkan ruang siber sebagai medium operasionalnya (Montasari, 2024). Seiring semakin terintegrasinya teknologi digital dalam kehidupan sehari-hari, pengawasan digital tidak lagi dipandang sebagai instrumen keamanan yang bersifat luar biasa (*exceptional measure*), melainkan telah berkembang menjadi mekanisme tata kelola yang rutin digunakan dalam penyelenggaraan pemerintahan modern.

Ekspansi pengawasan digital secara global semakin menguat setelah munculnya berbagai krisis keamanan dan kesehatan dalam dua dekade terakhir (Anstis & Sprenger, 2026). Pengungkapan praktik pengumpulan data intelijen secara massal, meningkatnya penggunaan perangkat lunak pengintai (*spyware*), serta pemanfaatan teknologi pelacakan digital selama pandemi COVID-19 menunjukkan bagaimana pengawasan berbasis teknologi semakin dinormalisasi dalam berbagai sistem politik (Papademetriou, 2023; Putra et al., 2024). Pemerintah umumnya membenarkan kebijakan tersebut sebagai respons yang diperlukan untuk menghadapi ancaman yang semakin kompleks dan sulit diprediksi. Namun demikian, banyak kalangan akademisi dan organisasi hak asasi manusia menilai bahwa normalisasi pengawasan digital berpotensi mengikis privasi individu, memperlemah akuntabilitas demokratis, dan mengancam perlindungan hak-hak fundamental warga negara (Deibert, 2023; Luo, 2024; Nuris Syawal et al., 2025). Kondisi ini melahirkan salah satu dilema tata kelola paling penting dalam era digital, yaitu bagaimana negara dapat meningkatkan keamanan tanpa mengorbankan kebebasan yang justru menjadi dasar legitimasi sistem demokrasi itu sendiri.

Perdebatan tersebut mencerminkan adanya pertarungan antara dua paradigma utama dalam studi keamanan dan hak asasi manusia. Paradigma keamanan (*security paradigm*) berangkat dari asumsi bahwa ancaman kontemporer memiliki karakter yang semakin kompleks, lintas batas, dan sulit dideteksi melalui mekanisme konvensional (Singh, 2024). Oleh karena itu, negara memerlukan kapasitas pengawasan yang lebih luas untuk mengidentifikasi potensi ancaman sebelum ancaman tersebut berkembang menjadi risiko nyata. Dalam perspektif ini, perluasan kewenangan pengawasan dianggap sebagai langkah yang sah dan diperlukan untuk menjaga stabilitas nasional, ketertiban publik, dan keselamatan masyarakat (Daah et al., 2024; Li, 2025).

Sebaliknya, paradigma hak asasi manusia (*human rights paradigm*) menekankan bahwa perluasan pengawasan digital dapat mengubah hubungan antara negara dan warga negara secara fundamental. Pemantauan terhadap komunikasi pribadi, aktivitas media sosial, data lokasi, serta berbagai bentuk jejak digital lainnya berpotensi menciptakan efek jera (*chilling effect*) terhadap kebebasan berekspresi, kebebasan berkumpul, dan partisipasi politik (Alrahamneh et al., 2026; Singh, 2024). Lebih jauh lagi, sistem pengawasan modern sering kali beroperasi melalui infrastruktur teknologi yang kompleks dan kurang transparan sehingga menyulitkan pengawasan publik maupun mekanisme akuntabilitas. Dalam kondisi demikian, pengawasan yang pada awalnya dirancang sebagai instrumen keamanan dapat berkembang menjadi alat kontrol sosial yang mengancam prinsip-prinsip demokrasi dan supremasi hukum.

Dalam perspektif hukum hak asasi manusia internasional, hak atas privasi merupakan hak fundamental yang dijamin dalam berbagai instrumen internasional, termasuk Pasal 17 *International Covenant on Civil and Political Rights* (ICCPR) (Siryon, 2025). Ketentuan tersebut menegaskan bahwa tidak seorang pun boleh menjadi sasaran campur tangan yang sewenang-wenang atau melawan hukum terhadap kehidupan pribadinya. Meskipun demikian, hukum internasional juga mengakui bahwa negara dapat membatasi hak-hak tertentu untuk tujuan yang sah, termasuk keamanan nasional. Namun, pembatasan tersebut harus memenuhi prinsip legalitas, kebutuhan (*necessity*), proporsionalitas (*proportionality*), dan akuntabilitas (*accountability*) (Abdelhameed, 2025; Weber, 2024). Dengan demikian, persoalan utama bukan terletak pada keberadaan pengawasan digital itu sendiri, melainkan pada bagaimana negara membangun kerangka hukum dan kelembagaan yang mampu mencegah penyalahgunaan kewenangan atas nama keamanan.

Perdebatan mengenai hubungan antara keamanan dan kebebasan sipil menjadi semakin penting dalam konteks Asia Tenggara. Kawasan ini merupakan salah satu pusat pertumbuhan ekonomi digital tercepat di dunia, ditandai dengan meningkatnya penetrasi internet, berkembangnya layanan keuangan digital, serta adopsi teknologi digital dalam berbagai sektor pemerintahan (Thompson, 2023). Pada saat yang sama, negara-negara di kawasan ini menghadapi berbagai ancaman keamanan baru, seperti serangan siber terhadap infrastruktur kritis, radikalisasi daring, manipulasi informasi digital, serta kejahatan transnasional berbasis teknologi. Untuk merespons tantangan tersebut, pemerintah di berbagai negara Asia Tenggara semakin memperluas penggunaan instrumen pengawasan digital sebagai bagian dari strategi keamanan nasional dan tata kelola digital (Caballero-Anthony & Emmers, 2022).

Menariknya, meskipun menghadapi tantangan keamanan yang relatif serupa, negara-negara Asia Tenggara menunjukkan variasi yang cukup besar dalam merancang dan menerapkan kebijakan pengawasan digital. Sebagian negara mengembangkan regulasi yang relatif menekankan perlindungan data pribadi, pengawasan yudisial, dan transparansi penggunaan kewenangan pengawasan. Sebaliknya, negara lain memberikan ruang yang lebih luas bagi pemerintah untuk melakukan pemantauan terhadap aktivitas digital masyarakat (Patil et al., 2025). Perbedaan tersebut menjadi menarik karena negara-negara tersebut beroperasi dalam lingkungan regional yang secara formal mengakui pentingnya perlindungan hak asasi manusia (Fiero & Beier, 2022). Dengan demikian, muncul pertanyaan mendasar: mengapa negara-negara yang berada dalam kerangka normatif regional yang sama menghasilkan kebijakan pengawasan digital yang sangat berbeda?

Pertanyaan tersebut menjadi semakin relevan ketika dikaitkan dengan karakteristik unik ASEAN sebagai organisasi regional. Di satu sisi, ASEAN telah menunjukkan komitmen terhadap perlindungan hak asasi manusia melalui ASEAN Human Rights Declaration (AHRD) dan pembentukan berbagai mekanisme kelembagaan yang berkaitan dengan promosi hak asasi manusia (Noh, 2022; Shope & Chang, 2022). Di sisi lain, ASEAN tetap mempertahankan prinsip *non-interference* dan penghormatan

terhadap kedaulatan negara sebagai fondasi utama kerja sama regional. Akibatnya, kawasan Asia Tenggara memperlihatkan paradoks normatif yang menarik. Negara-negara anggota secara kolektif mendukung prinsip-prinsip hak asasi manusia, tetapi pada saat yang sama tetap memiliki keleluasaan yang besar dalam menentukan bagaimana prinsip-prinsip tersebut diterapkan dalam sistem hukum nasional masing-masing (Häbel et al., 2022). Paradoks ini terlihat secara jelas dalam tata kelola pengawasan digital yang mempertemukan kepentingan keamanan, kedaulatan negara, dan perlindungan hak asasi manusia dalam satu arena kebijakan yang sama.

Literatur mengenai pengawasan digital, keamanan, dan hak asasi manusia telah berkembang secara signifikan dalam beberapa tahun terakhir. Kajian dalam bidang *surveillance studies* menunjukkan bagaimana perkembangan teknologi memperluas kapasitas negara dalam melakukan pemantauan terhadap masyarakat (Kasinathan et al., 2022; Mohsan et al., 2023). Sementara itu, kajian keamanan menjelaskan bagaimana ancaman digital dikonstruksikan sebagai ancaman eksistensial yang memerlukan respons kebijakan yang luar biasa (Jovanović, 2026; Nemorin et al., 2023). Di sisi lain, penelitian mengenai hak asasi manusia menyoroti implikasi pengawasan digital terhadap privasi, kebebasan sipil, dan akuntabilitas demokratis (Bocquet, 2025).

Meskipun demikian, literatur yang ada masih memiliki sejumlah keterbatasan. Pertama, sebagian besar penelitian masih didominasi oleh pengalaman negara-negara demokrasi liberal di Amerika Utara dan Eropa sehingga menghasilkan bias geografis dalam pengembangan teori pengawasan digital. Kedua, penelitian mengenai Asia Tenggara umumnya bersifat terfragmentasi dan lebih banyak berfokus pada studi kasus negara tertentu sehingga belum mampu menjelaskan pola tata kelola pengawasan digital di tingkat kawasan. Ketiga, sebagian besar studi cenderung menggunakan pendekatan keamanan atau hak asasi manusia secara terpisah, sehingga belum banyak menjelaskan bagaimana kedua logika tersebut berinteraksi dalam kawasan yang menjunjung tinggi prinsip kedaulatan seperti ASEAN.

Keterbatasan tersebut menunjukkan adanya kesenjangan penelitian yang penting. Hingga saat ini, masih terdapat pemahaman yang terbatas mengenai bagaimana proses sekritisasi ancaman digital berinteraksi dengan mekanisme tata kelola hak asasi manusia dalam membentuk kebijakan pengawasan digital di Asia Tenggara. Selain itu, masih sedikit penelitian yang menjelaskan mengapa negara-negara yang berada dalam kerangka normatif regional yang sama menghasilkan tingkat perlindungan hak asasi manusia yang berbeda dalam regulasi pengawasan digital mereka. Akibatnya, mekanisme yang menjelaskan hubungan antara keamanan nasional, kedaulatan negara, dan perlindungan hak asasi manusia dalam tata kelola digital kawasan masih belum dipahami secara memadai. Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk menganalisis implikasi hak asasi manusia dari kebijakan pengawasan digital di Asia Tenggara melalui pendekatan studi hukum komparatif regional. Dengan memanfaatkan perspektif *Securitization Theory* dan *Human Rights Governance*, penelitian ini mengkaji bagaimana negara-negara ASEAN mengonstruksikan ancaman

digital, membentuk kewenangan pengawasan negara, serta mengembangkan mekanisme perlindungan terhadap kebebasan sipil.

Penelitian ini berargumen bahwa variasi tata kelola pengawasan digital di Asia Tenggara ditentukan oleh interaksi antara tingkat sekuritisasi ancaman digital dan kekuatan mekanisme tata kelola hak asasi manusia di masing-masing negara. Ketika ancaman digital dikonstruksikan sebagai ancaman keamanan yang sangat mendesak dan mekanisme akuntabilitas relatif lemah, kebijakan pengawasan cenderung didominasi oleh kepentingan keamanan. Sebaliknya, ketika mekanisme perlindungan hak asasi manusia, pengawasan yudisial, dan kontrol kelembagaan lebih kuat, praktik pengawasan digital cenderung lebih terkendali dan sejalan dengan prinsip-prinsip hak asasi manusia. Penelitian ini memberikan tiga kontribusi utama. Pertama, penelitian ini memperluas kajian sekuritisasi dengan menunjukkan bagaimana lingkungan normatif regional memengaruhi institusionalisasi praktik keamanan dalam bentuk regulasi pengawasan digital. Kedua, penelitian ini memperkaya literatur tata kelola hak asasi manusia dengan menjelaskan kondisi yang memungkinkan perlindungan hak dapat membatasi perluasan kewenangan pengawasan negara. Ketiga, penelitian ini mengembangkan kerangka komparatif untuk memahami variasi tata kelola pengawasan digital di Asia Tenggara sehingga dapat mengisi kekosongan dalam literatur hukum dan tata kelola digital kawasan.

Penelitian ini menegaskan bahwa tantangan utama tata kelola digital di Asia Tenggara bukanlah memilih antara keamanan nasional dan kebebasan sipil, melainkan membangun kerangka hukum yang mampu menjamin keduanya secara bersamaan. Keberhasilan negara-negara ASEAN dalam mencapai keseimbangan tersebut akan menentukan kualitas perlindungan hak asasi manusia sekaligus legitimasi tata kelola digital di kawasan pada masa mendatang.

## **II. METODOLOGI**

### *A. Research Design*

Penelitian ini menggunakan desain penelitian hukum kualitatif (*qualitative legal research*) dengan pendekatan studi hukum komparatif regional (*comparative regional legal study*) untuk menganalisis implikasi hak asasi manusia dari kebijakan pengawasan digital di kawasan Asia Tenggara. Pendekatan komparatif dipilih karena memungkinkan peneliti untuk mengidentifikasi persamaan, perbedaan, dan pola regulasi pengawasan digital di berbagai negara yang berada dalam lingkungan regional yang sama, tetapi memiliki sistem hukum, sistem politik, dan tingkat perlindungan hak asasi manusia yang berbeda. Melalui pendekatan ini, penelitian berupaya memahami bagaimana negara-negara ASEAN menyeimbangkan kepentingan keamanan nasional dengan perlindungan kebebasan sipil dalam era transformasi digital. Penelitian ini menerapkan metode hukum normatif-komparatif (*normative comparative legal research*) yang berfokus pada analisis terhadap peraturan perundang-undangan, dokumen kebijakan, instrumen hak asasi manusia internasional, serta berbagai regulasi yang berkaitan dengan pengawasan digital. Pendekatan ini dipilih karena permasalahan yang diteliti berkaitan dengan

konstruksi norma hukum, kewenangan negara, dan mekanisme perlindungan hak asasi manusia dalam tata kelola pengawasan digital.

### B. Theoretical Framework

Penelitian ini menggunakan dua kerangka teoritis utama, yaitu *Securitization Theory* dan *Human Rights Governance*. *Securitization Theory* digunakan untuk menjelaskan bagaimana negara mengonstruksikan ancaman digital sebagai ancaman keamanan nasional yang memerlukan respons luar biasa melalui perluasan kewenangan pengawasan digital. Teori ini membantu memahami proses legitimasi kebijakan pengawasan yang dilakukan pemerintah atas nama keamanan. Sementara itu, *Human Rights Governance* digunakan untuk mengevaluasi sejauh mana sistem hukum dan kelembagaan yang ada mampu membatasi penggunaan kewenangan pengawasan negara agar tetap sejalan dengan prinsip-prinsip hak asasi manusia. Kerangka ini menekankan pentingnya prinsip legalitas, kebutuhan (*necessity*), proporsionalitas (*proportionality*), transparansi (*transparency*), dan akuntabilitas (*accountability*) dalam penyelenggaraan pengawasan digital. Integrasi kedua perspektif tersebut memungkinkan penelitian untuk menjelaskan hubungan antara proses sekuritisasi ancaman digital, pembentukan regulasi pengawasan, dan tingkat perlindungan hak asasi manusia di negara-negara Asia Tenggara.

### C. Case Selection

Penelitian ini memilih enam negara anggota ASEAN sebagai objek analisis, yaitu Indonesia, Singapura, Malaysia, Thailand, Vietnam, dan Filipina. Pemilihan negara dilakukan menggunakan teknik purposive sampling berdasarkan beberapa pertimbangan. Pertama, negara-negara tersebut memiliki regulasi yang secara eksplisit mengatur pengawasan digital, keamanan siber, atau akses negara terhadap data elektronik. Kedua, tersedia dokumen hukum dan kebijakan yang memadai untuk dianalisis secara komparatif. Ketiga, terdapat variasi yang signifikan dalam sistem politik, tradisi hukum, dan tingkat perlindungan hak asasi manusia sehingga memungkinkan identifikasi pola tata kelola pengawasan digital yang lebih luas di kawasan ASEAN.

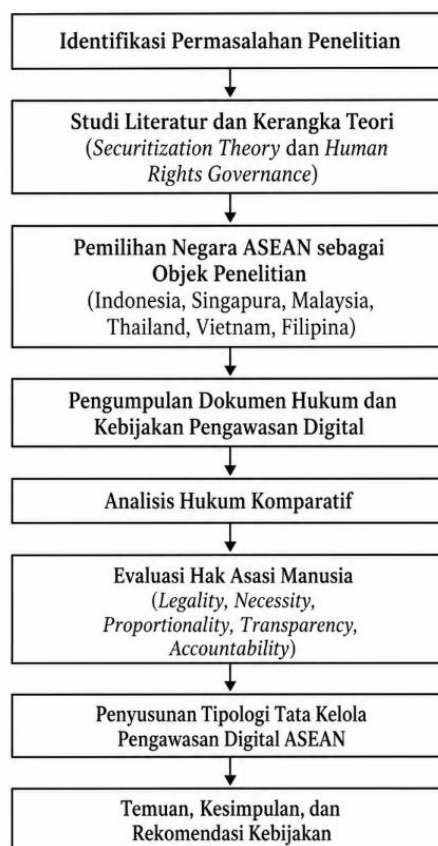
**Tabel 1. Comparative Analytical Framework**

| Dimensi Analisis                 | Indikator                                                                              | Tujuan Analisis                                                  |
|----------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Orientasi Keamanan               | Undang-undang keamanan nasional, regulasi keamanan siber, narasi ancaman digital       | Mengukur tingkat sekuritisasi ancaman digital                    |
| Kewenangan Pengawasan            | Penyadapan komunikasi, akses data elektronik, pemantauan aktivitas digital             | Menilai ruang lingkup kewenangan negara dalam pengawasan digital |
| Mekanisme Pengawasan Hukum       | Persetujuan pengadilan, pengawasan legislatif, lembaga independen                      | Mengevaluasi akuntabilitas dan pengawasan kelembagaan            |
| Perlindungan Hak Asasi Manusia   | Hak privasi, kebebasan berekspresi, perlindungan data pribadi                          | Mengukur tingkat perlindungan hak asasi manusia                  |
| Transparansi dan Akuntabilitas   | Pelaporan publik, mekanisme pengaduan, akses informasi                                 | Menilai kualitas tata kelola pengawasan digital                  |
| Kepatuhan terhadap Prinsip ASEAN | Kesesuaian dengan ASEAN Human Rights Declaration (AHRD) dan instrumen regional lainnya | Menilai pengaruh norma regional ASEAN terhadap regulasi nasional |

Sumber : Olahan Peneliti, 2026

#### D. Data Collection

Data penelitian diperoleh melalui studi dokumen (*documentary research*). Sumber data primer meliputi konstitusi, undang-undang keamanan siber, undang-undang perlindungan data pribadi, regulasi komunikasi elektronik, regulasi intelijen, serta berbagai kebijakan pemerintah yang berkaitan dengan pengawasan digital. Sementara itu, sumber data sekunder mencakup artikel jurnal internasional bereputasi, buku akademik, laporan organisasi internasional, dokumen ASEAN, laporan lembaga hak asasi manusia, dan publikasi lembaga penelitian yang relevan. Pengumpulan data dilakukan secara sistematis dengan memanfaatkan basis data hukum nasional, portal resmi pemerintah, dokumen ASEAN, serta artikel ilmiah yang terindeks *Scopus* dan *Web of Science*. Penggunaan sumber-sumber tersebut bertujuan untuk menjamin validitas dan kredibilitas data yang digunakan dalam penelitian.



**Gambar 1. Research Flowchart.** Sumber : Olahan Peneliti, 2026

#### E. Data Analysis

Analisis data dilakukan menggunakan metode analisis hukum komparatif kualitatif (*qualitative comparative legal analysis*) yang terdiri atas tiga tahapan utama. Tahap pertama adalah analisis intra-negara (*within-case analysis*), yaitu mengidentifikasi karakteristik regulasi pengawasan digital pada masing-masing negara yang menjadi objek penelitian. Analisis ini mencakup dasar hukum, bentuk kewenangan pengawasan, mekanisme akuntabilitas, serta instrumen perlindungan hak asasi manusia yang tersedia. Tahap kedua adalah analisis lintas negara (*cross-case comparison*) untuk membandingkan persamaan dan perbedaan regulasi pengawasan digital di antara negara-negara

ASEAN yang diteliti. Melalui tahap ini dapat diidentifikasi pola tata kelola pengawasan digital yang berkembang di kawasan.

Tahap ketiga adalah interpretasi teoretis dengan menggunakan perspektif *Securitization Theory* dan *Human Rights Governance*. Analisis ini bertujuan menjelaskan faktor-faktor yang menyebabkan variasi tingkat perlindungan hak asasi manusia dalam kebijakan pengawasan digital antarnegara. Dalam melakukan evaluasi, penelitian menggunakan lima indikator utama yang berasal dari standar hukum hak asasi manusia internasional, yaitu: Legalitas (*legality*), Kebutuhan (*necessity*), Proporsionalitas (*proportionality*), Transparansi (*transparency*), dan Akuntabilitas (*accountability*). Kelima indikator tersebut digunakan sebagai parameter untuk menilai kesesuaian kebijakan pengawasan digital dengan prinsip-prinsip hak asasi manusia internasional.

#### F. *Research Validity and Trustworthiness*

Untuk meningkatkan validitas penelitian, digunakan teknik triangulasi sumber (*source triangulation*) dengan membandingkan berbagai jenis dokumen hukum, dokumen kebijakan, literatur akademik, dan instrumen hak asasi manusia internasional. Selain itu, validitas analisis diperkuat melalui perbandingan sistematis antarnegara menggunakan indikator evaluasi yang sama sehingga menghasilkan analisis yang konsisten dan dapat direplikasi. Pendekatan ini memungkinkan penelitian menghasilkan temuan yang lebih komprehensif dan memiliki tingkat keandalan yang tinggi dalam menjelaskan variasi tata kelola pengawasan digital di kawasan ASEAN.

#### G. *Ethical Considerations*

Penelitian ini tidak melibatkan partisipan manusia, wawancara, survei, maupun pengumpulan data pribadi sehingga tidak menimbulkan risiko etis secara langsung. Seluruh data yang digunakan berasal dari dokumen publik yang tersedia secara legal dan dapat diakses oleh masyarakat. Meskipun demikian, penelitian tetap dilaksanakan berdasarkan prinsip integritas akademik, objektivitas ilmiah, transparansi metodologis, dan penghormatan terhadap hak kekayaan intelektual dalam penggunaan sumber-sumber penelitian.

### III. HASIL DAN DISKUSI

#### Hasil

Analisis komparatif terhadap kebijakan pengawasan digital di Indonesia, Singapura, Malaysia, Thailand, Vietnam, dan Filipina menunjukkan bahwa seluruh negara ASEAN yang diteliti telah mengembangkan kerangka regulasi yang memberikan kewenangan kepada negara untuk melakukan pengawasan terhadap aktivitas digital masyarakat. Namun demikian, terdapat variasi yang signifikan dalam tingkat kewenangan pengawasan, mekanisme akuntabilitas, perlindungan data pribadi, dan jaminan hak asasi manusia yang menyertainya. Variasi tersebut menunjukkan bahwa meskipun negara-negara ASEAN menghadapi ancaman keamanan digital yang relatif serupa, respons regulasi yang dihasilkan tidak bersifat homogen. Hasil penelitian menunjukkan bahwa Singapura, Malaysia,

Thailand, dan Filipina telah mengembangkan sistem perlindungan data pribadi yang relatif lebih matang dibandingkan Indonesia dan Vietnam. Negara-negara tersebut memiliki regulasi perlindungan data yang lebih terstruktur, lembaga pengawas yang lebih jelas, serta mekanisme pengaduan yang memungkinkan individu memperoleh perlindungan hukum ketika hak privasinya dilanggar. Sebaliknya, Indonesia masih berada pada fase konsolidasi kelembagaan pasca pemberlakuan Undang-Undang Perlindungan Data Pribadi, sementara Vietnam tetap mempertahankan pendekatan yang memberikan ruang yang luas bagi negara untuk melakukan pengawasan atas dasar keamanan nasional.

Temuan lainnya menunjukkan bahwa seluruh negara yang diteliti menggunakan narasi ancaman digital sebagai dasar legitimasi perluasan kewenangan pengawasan. Ancaman tersebut mencakup terorisme, radikalisme daring, serangan siber terhadap infrastruktur kritis, penyebaran disinformasi, serta kejahatan transnasional berbasis teknologi. Meskipun demikian, tingkat sekuritisasi ancaman digital menunjukkan perbedaan yang cukup signifikan. Vietnam dan Indonesia menunjukkan tingkat sekuritisasi yang lebih tinggi dibandingkan negara lainnya, sementara Filipina dan Thailand relatif lebih menekankan keseimbangan antara kepentingan keamanan dan perlindungan hak privasi.

**Tabel 2. Comparative Characteristics of Digital Surveillance Governance in ASEAN**

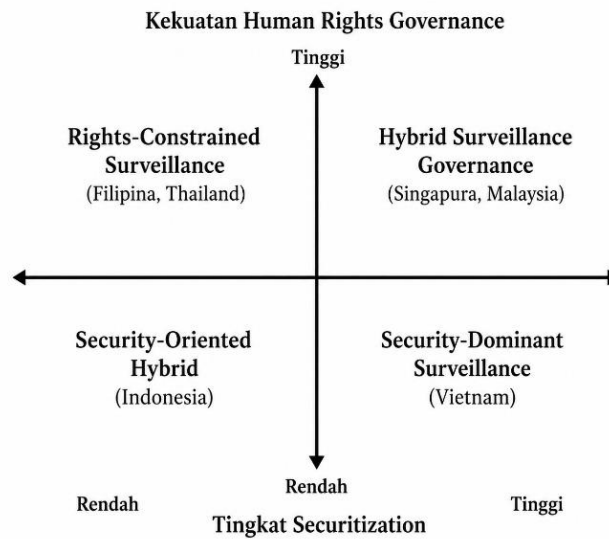
| Negara      | Tingkat Securitization | Perlindungan Data Pribadi | Pengawasan Yudisial | Transparansi | Kategori Tata Kelola                   |
|-------------|------------------------|---------------------------|---------------------|--------------|----------------------------------------|
| Indonesia   | Tinggi                 | Sedang                    | Rendah–Sedang       | Rendah       | <i>Security-Oriented Hybrid</i>        |
| Singapore   | Tinggi                 | Tinggi                    | Sedang              | Sedang       | <i>Hybrid Surveillance Governance</i>  |
| Malaysia    | Sedang                 | Sedang                    | Sedang              | Sedang       | <i>Hybrid Surveillance Governance</i>  |
| Thailand    | Sedang                 | Tinggi                    | Sedang              | Sedang       | <i>Rights-Constrained Surveillance</i> |
| Philippines | Sedang                 | Tinggi                    | Tinggi              | Sedang       | <i>Rights-Constrained Surveillance</i> |
| Vietnam     | Sangat Tinggi          | Rendah                    | Rendah              | Rendah       | <i>Security-Dominant Surveillance</i>  |

Sumber : Olahan Peneliti, 2026

Berdasarkan hasil perbandingan di Tabel 2, penelitian ini mengidentifikasi empat pola utama tata kelola pengawasan digital di kawasan ASEAN. Pertama, *Security-Dominant Surveillance*, yaitu model yang memberikan prioritas utama pada keamanan nasional dengan tingkat pembatasan yang relatif rendah terhadap kewenangan negara. Kedua, *Security-Oriented Hybrid*, yaitu model yang mulai mengintegrasikan perlindungan hak asasi manusia tetapi masih didominasi oleh kepentingan keamanan. Ketiga, *Hybrid Surveillance Governance*, yaitu model yang relatif menyeimbangkan kebutuhan keamanan dengan perlindungan hak privasi. Keempat, *Rights-Constrained Surveillance*, yaitu model yang menempatkan perlindungan hak asasi manusia sebagai batas utama dalam penggunaan kewenangan pengawasan negara.

Temuan tersebut menunjukkan bahwa variasi tata kelola pengawasan digital di Asia Tenggara tidak dapat dijelaskan hanya berdasarkan tingkat ancaman keamanan yang dihadapi masing-masing negara. Sebaliknya, hasil penelitian menunjukkan bahwa variasi tersebut juga dipengaruhi oleh kapasitas

kelembagaan, tradisi hukum, mekanisme pengawasan independen, serta tingkat komitmen terhadap perlindungan hak asasi manusia.



**Gambar 2. ASEAN Surveillance Governance Typology.** Sumber : Olahan Peneliti, 2026

## Diskusi

Temuan penelitian ini memberikan dukungan empiris terhadap asumsi utama *Securitization Theory* yang menyatakan bahwa suatu isu dapat memperoleh status prioritas kebijakan ketika dikonstruksikan sebagai ancaman eksistensial terhadap negara. Dalam konteks Asia Tenggara, ancaman digital berhasil disekuritisasi melalui narasi mengenai keamanan siber, stabilitas nasional, kedaulatan digital, dan perlindungan infrastruktur kritis. Proses sekuritisasi tersebut memungkinkan pemerintah memperoleh legitimasi yang lebih besar untuk memperluas kewenangan pengawasan digital (Burton, 2023; Onditi, 2022). Namun demikian, penelitian ini menunjukkan bahwa keberhasilan sekuritisasi tidak secara otomatis menghasilkan bentuk tata kelola yang seragam di seluruh kawasan.

Temuan ini memperluas literatur *Securitization Theory* dengan menunjukkan bahwa hasil akhir dari proses sekuritisasi sangat dipengaruhi oleh kapasitas tata kelola hak asasi manusia yang berkembang dalam masing-masing negara (Bhat & Shahid, 2024; Buranajaroenkij & Hayes, 2025). Dengan kata lain, ancaman digital yang dikonstruksikan secara serupa dapat menghasilkan konsekuensi regulasi yang berbeda ketika berinteraksi dengan institusi hukum dan mekanisme akuntabilitas yang berbeda. Oleh karena itu, penelitian ini mengusulkan bahwa hubungan antara sekuritisasi dan perluasan kewenangan negara tidak bersifat linear, melainkan dimediasi oleh kekuatan institusi perlindungan hak asasi manusia.

Selain itu, penelitian ini juga memberikan kontribusi terhadap literatur *Human Rights Governance*. Sebagian besar penelitian sebelumnya menekankan pentingnya keberadaan regulasi perlindungan data pribadi sebagai indikator utama perlindungan hak privasi. Namun, hasil penelitian ini menunjukkan bahwa keberadaan regulasi formal saja tidak cukup untuk menjamin perlindungan hak asasi manusia. Efektivitas perlindungan hak sangat bergantung pada keberadaan lembaga pengawas independen,

mekanisme pengawasan yudisial, transparansi kebijakan, serta akses masyarakat terhadap upaya hukum ketika terjadi pelanggaran hak. Dengan demikian, tata kelola hak asasi manusia harus dipahami sebagai kombinasi antara norma hukum dan kapasitas kelembagaan yang mendukung implementasinya. Temuan paling penting dalam penelitian ini adalah munculnya apa yang dapat disebut sebagai *ASEAN Surveillance Paradox*. Di satu sisi, negara-negara ASEAN secara kolektif mengakui pentingnya perlindungan hak asasi manusia melalui berbagai instrumen regional. Di sisi lain, prinsip non-interference dan penghormatan terhadap kedaulatan negara memberikan ruang yang sangat luas bagi masing-masing negara untuk menentukan batas-batas pengawasan digitalnya sendiri. Akibatnya, terjadi konvergensi normatif pada tingkat regional tetapi divergensi implementatif pada tingkat nasional.

Paradoks tersebut menjelaskan mengapa negara-negara yang berada dalam kerangka normatif regional yang sama dapat menghasilkan model tata kelola pengawasan digital yang sangat berbeda. Temuan ini mengisi kesenjangan penelitian yang selama ini belum mampu menjelaskan variasi kebijakan pengawasan digital di kawasan Asia Tenggara (Gustafsson et al., 2023; Schilling-Vacaflor & Gustafsson, 2024). Dengan mengintegrasikan perspektif *Securitization Theory* dan *Human Rights Governance*, penelitian ini menunjukkan bahwa variasi tersebut merupakan hasil interaksi antara tingkat sekuritisasi ancaman digital dan kekuatan mekanisme perlindungan hak asasi manusia di tingkat nasional. Secara teoretis, penelitian ini menghasilkan kontribusi berupa *ASEAN Surveillance Governance Typology* yang mengklasifikasikan tata kelola pengawasan digital ke dalam empat kategori utama, yaitu *Security-Dominant Surveillance*, *Security-Oriented Hybrid*, *Hybrid Surveillance Governance*, dan *Rights-Constrained Surveillance*. Tipologi ini menawarkan kerangka analitis baru untuk memahami variasi kebijakan pengawasan digital di Asia Tenggara dan dapat digunakan sebagai dasar untuk penelitian komparatif di kawasan lain.

Secara praktis, hasil penelitian menunjukkan bahwa peningkatan keamanan digital tidak harus dilakukan melalui perluasan kewenangan negara yang tidak terkendali. Negara-negara ASEAN dapat memperkuat keamanan nasional sekaligus mempertahankan legitimasi demokratis dengan mengembangkan mekanisme pengawasan independen, meningkatkan transparansi penggunaan teknologi pengawasan, memperkuat perlindungan data pribadi, dan memastikan bahwa setiap pembatasan terhadap hak-hak individu memenuhi prinsip legalitas, kebutuhan, proporsionalitas, dan akuntabilitas. Dengan demikian, masa depan tata kelola digital di Asia Tenggara tidak ditentukan oleh pilihan antara keamanan atau kebebasan, melainkan oleh kemampuan negara untuk membangun keseimbangan yang berkelanjutan antara keduanya.

#### **IV. KESIMPULAN**

Penelitian ini menganalisis implikasi hak asasi manusia dari kebijakan pengawasan digital di Asia Tenggara melalui pendekatan studi hukum komparatif regional terhadap enam negara ASEAN, yaitu Indonesia, Singapura, Malaysia, Thailand, Vietnam, dan Filipina. Hasil penelitian menunjukkan

bahwa seluruh negara yang dianalisis telah mengembangkan kerangka regulasi yang memungkinkan negara melakukan pengawasan terhadap aktivitas digital masyarakat sebagai respons terhadap meningkatnya ancaman keamanan siber, terorisme digital, disinformasi, dan berbagai bentuk kejahatan transnasional berbasis teknologi. Namun demikian, penelitian ini menemukan bahwa tingkat kewenangan pengawasan, mekanisme akuntabilitas, dan perlindungan hak asasi manusia yang diterapkan oleh masing-masing negara menunjukkan variasi yang signifikan. Berdasarkan perspektif *Securitization Theory*, penelitian ini membuktikan bahwa ancaman digital telah berhasil dikonstruksikan sebagai ancaman keamanan nasional yang memerlukan respons kebijakan luar biasa. Proses sekuritisasi tersebut memberikan legitimasi bagi negara untuk memperluas kapasitas pengawasan digital melalui berbagai instrumen hukum dan kebijakan. Akan tetapi, temuan penelitian menunjukkan bahwa keberhasilan proses sekuritisasi tidak secara otomatis menghasilkan model tata kelola pengawasan yang seragam. Sebaliknya, bentuk dan intensitas pengawasan digital sangat dipengaruhi oleh kapasitas kelembagaan, tradisi hukum, tingkat demokratisasi, dan kekuatan mekanisme perlindungan hak asasi manusia yang berkembang dalam masing-masing negara.

Penelitian ini juga memperlihatkan bahwa efektivitas perlindungan hak asasi manusia dalam tata kelola pengawasan digital tidak hanya ditentukan oleh keberadaan regulasi perlindungan data pribadi, tetapi juga oleh keberadaan lembaga pengawas independen, pengawasan yudisial, transparansi kebijakan, dan akses masyarakat terhadap mekanisme pemulihan hukum. Negara-negara yang memiliki institusi akuntabilitas yang lebih kuat cenderung mampu membatasi penggunaan kewenangan pengawasan secara lebih proporsional dibandingkan negara yang menempatkan keamanan nasional sebagai pertimbangan dominan dalam pembentukan kebijakan digital. Kontribusi teoretis utama penelitian ini adalah pengembangan *ASEAN Surveillance Governance Typology*, yang mengklasifikasikan tata kelola pengawasan digital ke dalam empat kategori utama, yaitu *Security-Dominant Surveillance*, *Security-Oriented Hybrid*, *Hybrid Surveillance Governance*, dan *Rights-Constrained Surveillance*. Tipologi ini menunjukkan bahwa variasi tata kelola pengawasan digital di Asia Tenggara merupakan hasil interaksi antara tingkat sekuritisasi ancaman digital dan kekuatan mekanisme *Human Rights Governance*. Temuan ini memperluas literatur mengenai sekuritisasi dengan menunjukkan bahwa dampak sekuritisasi terhadap perluasan kewenangan negara dimediasi oleh kapasitas institusional perlindungan hak asasi manusia.

Selain itu, penelitian ini mengidentifikasi fenomena yang disebut sebagai *ASEAN Surveillance Paradox*, yaitu kondisi ketika negara-negara ASEAN secara kolektif mengakui pentingnya perlindungan hak asasi manusia melalui berbagai instrumen regional, tetapi pada saat yang sama tetap mempertahankan tingkat otonomi yang tinggi dalam menentukan kebijakan pengawasan digital nasional. Paradoks ini menghasilkan konvergensi normatif pada tingkat regional dan divergensi implementatif pada tingkat nasional. Dengan demikian, variasi kebijakan pengawasan digital di Asia Tenggara tidak hanya mencerminkan perbedaan tingkat ancaman keamanan, tetapi juga perbedaan

interpretasi terhadap hubungan antara keamanan nasional, kedaulatan negara, dan perlindungan hak asasi manusia. Secara praktis, penelitian ini menegaskan bahwa keamanan nasional dan kebebasan sipil tidak harus diposisikan sebagai tujuan yang saling bertentangan. Penguatan keamanan digital dapat berjalan beriringan dengan perlindungan hak asasi manusia apabila didukung oleh prinsip legalitas, kebutuhan, proporsionalitas, transparansi, dan akuntabilitas yang kuat. Oleh karena itu, negara-negara ASEAN perlu memperkuat harmonisasi standar perlindungan data pribadi, meningkatkan independensi lembaga pengawas, memperluas pengawasan yudisial terhadap aktivitas pengawasan digital, serta mengembangkan mekanisme akuntabilitas yang lebih transparan dan partisipatif.

Meskipun demikian, penelitian ini memiliki keterbatasan karena berfokus pada analisis normatif terhadap regulasi dan kebijakan yang berlaku tanpa mengukur secara langsung implementasi praktik pengawasan digital di lapangan. Oleh sebab itu, penelitian selanjutnya disarankan untuk mengombinasikan pendekatan hukum komparatif dengan studi empiris, wawancara kebijakan, atau analisis institusional guna memperoleh pemahaman yang lebih mendalam mengenai efektivitas perlindungan hak asasi manusia dalam praktik pengawasan digital di kawasan Asia Tenggara. Dengan demikian, penelitian masa depan dapat memperkaya pemahaman mengenai dinamika hubungan antara keamanan, teknologi, dan hak asasi manusia dalam tata kelola digital global yang terus berkembang.

## REFERENSI

- Abdelhameed, A. (2025). Cultural Values as a Gatekeeper in Malaysia's Human Rights Policy: Advocating for Inclusive International Instruments. *Journal of Politics and Law*, 18(4), 36. <https://doi.org/10.5539/jpl.v18n4p36>
- Alrahamneh, A., Murshed, A. A., & Alhalalmeh, E. (2026). Privacy vs. Surveillance: Balancing National Security and Human Rights in the Digital Age. *Studies in Systems, Decision and Control*, 227, 69–79. [https://doi.org/10.1007/978-3-031-95310-1\\_6](https://doi.org/10.1007/978-3-031-95310-1_6)
- Anstis, S., & Sprenger, J. (2026). Civil Society and Access to Justice: Challenges of Seeking Remedy in the Global Fight Against Spyware. *International Journal of Human Rights*. <https://doi.org/10.1080/13642987.2025.2603540>
- Bhat, M. A., & Shahid, R. (2024). Introduction: Mutual Attrition of Citizenship, Democracy and the Rule of Law in South and Southeast Asia. *Journal of Ethnic and Migration Studies*, 50(19), 4787–4808. <https://doi.org/10.1080/1369183X.2024.2376403>
- Bocquet, N. (2025). Caught Between Privacy and Surveillance: Explaining the Long-Term Stagnation of Data Protection Regulation in Liberal Democracies. *Regulation and Governance*. <https://doi.org/10.1111/rego.12656>
- Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict and Terrorism*, 46(12), 2426–2453. <https://doi.org/10.1080/1057610X.2021.1928887>
- Buranajaroenkij, D., & Hayes, M. (2025). The Securitization of Social Reintegration in Southern Thailand's Armed Conflict. *Conflict Resolution Quarterly*, 42(3), 425–435.

<https://doi.org/10.1002/crq.21458>

- Burton, J. (2023). Algorithmic Extremism? The Securitization of Artificial Intelligence (AI) and its Impact on Radicalism, Polarization and Political Violence. *Technology in Society*, 75. <https://doi.org/10.1016/j.techsoc.2023.102262>
- Caballero-Anthony, M., & Emmers, R. (2022). Keeping the Peace in Southeast Asia: ASEAN and the Quest for Positive Peace. *Pacific Review*, 35(6), 1079–1104. <https://doi.org/10.1080/09512748.2022.2075440>
- Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics (Switzerland)*, 13(5). <https://doi.org/10.3390/electronics13050865>
- Deibert, R. J. (2023). The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. *Foreign Affairs*, 102(1), 72–88.
- Fiero, A. W., & Beier, E. (2022). New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation. *Stanford Journal of International Law. Summer2022*, 58(2), 151–192. <https://web.s.ebscohost.com/ehost/detail/detail?vid=43&sid=84cbea20-4a76-4b13-8276-f7e1c6d77d8c%40redis&bdata=JkF1dGhUeXBIPXNzbyZzY29wZT1zaXRl#AN=158842953&db=a9h>
- Gustafsson, M. T., Schilling-Vacaflor, A., & Lenschow, A. (2023). The Politics of Supply Chain Regulations: Towards Foreign Corporate Accountability in the Area of Human Rights and the Environment? *Regulation and Governance*, 17(4), 853–869. <https://doi.org/10.1111/rego.12526>
- Häbel, S., Koff, H., & Adam, M. (2022). Normative Coherence for Development and Regionalism: Gender Equality in ASEAN's Migration Policies. *Development Policy Review*, 40(S1). <https://doi.org/10.1111/dpr.12618>
- Jovanović, S. M. (2026). Multiculturalism as a Veiled Vehicle for Global Right-Wing Ideologies: A Theoretical Reframing. *World Affairs*, 189(1). <https://doi.org/10.1002/waf2.70056>
- Kasinathan, P., Pugazhendhi, R., Elavarasan, R. M., Ramachandaramurthy, V. K., Ramanathan, V., Subramanian, S., Kumar, S., Nandhagopal, K., Raghavan, R. R. V., Rangasamy, S., Devendiran, R., & Alsharif, M. H. (2022). Realization of Sustainable Development Goals with Disruptive Technologies by Integrating Industry 5.0, Society 5.0, Smart Cities and Villages. *Sustainability (Switzerland)*, 14(22). <https://doi.org/10.3390/su142215258>
- Li, H. (2025). New Pathways for Paradigm Shifts in EU Foreign and Security Policy: from the Liberal International Order to Symbiotic Security Order. *Chinese Political Science Review*. <https://doi.org/10.1007/s41111-025-00320-3>
- Luo, Y. (2024). Paradigm Shift and Theoretical Implications for The Era of Global Disorder. *Journal of International Business Studies*, 55(2), 127–135. <https://doi.org/10.1057/s41267-023-00659-2>
- Matey, G. D. (2024). Non-state Actors and Technological Revolution: Organized Crime and International Terrorism. *Contributions to International Relations, Part F3536*, 89–106. [https://doi.org/10.1007/978-3-031-66750-3\\_7](https://doi.org/10.1007/978-3-031-66750-3_7)

- Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned Aerial Vehicles (Uavs): Practical Aspects, Applications, Open Challenges, Security Issues, and Future Trends. *Intelligent Service Robotics*, 16(1), 109–137. <https://doi.org/10.1007/s11370-022-00452-4>
- Montasari, R. (2024). Introduction: Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. *Advanced Sciences and Technologies for Security Applications, Part F2157*, 1–15. [https://doi.org/10.1007/978-3-031-50454-9\\_1](https://doi.org/10.1007/978-3-031-50454-9_1)
- Nemorin, S., Vlachidis, A., Ayerakwa, H. M., & Andriotis, P. (2023). AI Hyped? A Horizon Scan of Discourse on Artificial Intelligence in Education (AIED) and Development. *Learning, Media and Technology*, 48(1), 38–51. <https://doi.org/10.1080/17439884.2022.2095568>
- Noh, J. E. (2022). Review of Human Rights-Based Approaches to Development: Empirical Evidence from Developing Countries. *International Journal of Human Rights*, 26(5), 883–901. <https://doi.org/10.1080/13642987.2021.1981869>
- Nuris Syawal, I., Nazura Fadilla, N., & Author, C. (2025). The International Legal Framework and Social Justice: An Evaluation of the Effectiveness of Transnational Human Rights Instruments. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 3(3), 1276–1290. <https://doi.org/10.51903/4MF6XM54>
- Onditi, F. (2022). Securitization Versus Human Security: An Ontological Argument. *Human Security and Sustainable Development in East Africa*, 41–55. <https://doi.org/10.4324/9781003221081-3>
- Papademetriou, G. T. (2023). Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry. *Harvard Human Rights Journal*, 36, 191–221. <https://research.ebsco.com/linkprocessor/plink?id=37dfcedd-bdef-3fd7-b817-887588516015>
- Patil, A., Mishra, B., Chockalingam, S., Misra, S., & Kvalvik, P. (2025). Securing Financial Systems Through Data Sovereignty: A Systematic Review of Approaches and Regulations. *International Journal of Information Security*, 24(4). <https://doi.org/10.1007/s10207-025-01074-4>
- Putra, R. K., Kriswandaru, A. S., & Imaliya, T. (2024). Kajian Hukum Tata Negara terkait Pembatasan Kebebasan Berpendapat di Media Sosial di Era Pandemi COVID-19: Pendekatan Deskriptif Kualitatif. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 2(4), 857–872. <https://doi.org/10.51903/HAKIM.V2I4.2195>
- Schilling-Vacaflor, A., & Gustafsson, M. T. (2024). Towards More Sustainable Global Supply Chains? Company Compliance with new Human Rights and Environmental Due Diligence Laws. *Environmental Politics*, 33(3), 422–443. <https://doi.org/10.1080/09644016.2023.2221983>
- Shope, M. L., & Chang, W. C. (2022). Civil Society and Regional Human Rights Development in Asia: Lessons from the Asian Human Rights Court Simulation. *Indiana Journal of Global Legal Studies*, 29(1), 59–84.
- Singh, T. (2024). AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy. *Smart Innovation, Systems and Technologies*, 392 SIST, 703–717. [https://doi.org/10.1007/978-981-97-3690-4\\_53](https://doi.org/10.1007/978-981-97-3690-4_53)
- Siryon, S. S. (2025). Principles and Applications of the Right To Privacy: Evaluating International Perspectives and Laws. *LawFoyer International Journal of Doctrinal Legal Research*, 3(3), 897–

909. <https://doi.org/10.70183/lijdlr.2025.v03.116>

Thompson, M. R. (2023). The Paradoxes of “Vernacularised” Liberalism in Southeast Asia. *Asian Studies Review*, 47(1), 16–35. <https://doi.org/10.1080/10357823.2021.1940842>

Weber, A. (2024). Civil Liberties I (Freedom, Life, Liberty, Privacy). *Writing Constitutions: Volume 2: Fundamental Rights*, 107–150. [https://doi.org/10.1007/978-3-031-39622-9\\_4](https://doi.org/10.1007/978-3-031-39622-9_4)