Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://jhlg.rewangrencang.com/

CYBER SURVEILLANCE DALAM PENANGANAN TINDAK PIDANA TERORISME: ANTARA KEAMANAN NASIONAL DAN HAK PRIVASI

CYBER SURVEILLANCE IN HANDLING TERRORISM CRIMINAL ACTS: BETWEEN NATIONAL SECURITY AND PRIVACY RIGHTS

Khayrunaas Adhyaksa Mulyana

Universitas Padjadjaran

Korespondensi Penulis : khayrunaasam10@gmail.com

Citation Structure Recommendation :

Mulyana, Khayrunaas Adhyaksa. *Cyber Surveillance dalam Penanganan Tindak Pidana Terorisme: Antara Keamanan Nasional dan Hak Privasi*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).

ABSTRAK

Perkembangan teknologi digital mendorong perubahan pola tindak pidana terorisme yang semakin memanfaatkan ruang siber, sehingga negara menerapkan *cyber surveillance* sebagai instrumen untuk menjaga keamanan nasional. Namun, praktik tersebut berpotensi menimbulkan pelanggaran hak privasi sebagai hak asasi manusia yang dijamin oleh konstitusi. Penelitian ini menganalisis konsep dan praktik *cyber surveillance* dalam penanganan terorisme di Indonesia, kedudukan hak privasi dalam hukum nasional dan instrumen HAM, serta merumuskan model pengaturan ideal yang menyeimbangkan keamanan nasional dan hak privasi. Hasil penelitian menunjukan bahwa hak privasi dapat dibatasi oleh hukum namun perlu adanya regulasi yang komprehensif, proporsional dan akuntabel dalam penerapan *cyber surveillance*.

Kata Kunci: Cyber Surveillance, Hak Privasi, Keamanan Nasional, Terorisme

ABSTRACT

The development of digital technology has transformed terrorism into a cyber-based crime, prompting states to implement cyber surveillance as a tool to safeguard national security. However, such practices raise concerns regarding violations of privacy rights as fundamental human rights. This article examines the concept and practice of cyber surveillance in handling terrorism in Indonesia, the legal position of privacy rights under national law and human rights instruments, and proposes an ideal regulatory model to balance national security and privacy protection. The study concludes that the right to privacy can be limited by law, but there needs to be comprehensive, proportional and accountable regulations in the implementation of cyber surveillance.

Keywords: Cyber Surveillance, Privacy Rights, National Security, Terrorism

A. PENDAHULUAN

Secara terminologi, terorisme merupakan perbuatan kejahatan dengan menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas yang dapat menimbulkan korban yang bersifat massal atau menimbulkan kerusakan dan kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik atau gangguan keamanan.[1] Tindak pidana terorisme seringkali dilakukan secara berkelompok dan sistematik yang diawali oleh adanya perencanaan yang matang guna menyebabkan kehancuran yang eksesif. Dalam hukum positif Indonesia, terorisme dikualifikasikan sebagai kejahatan luar biasa (*extraordinary crime*) karena dampaknya yang serius terhadap keamanan nasional, ketertiban umum serta kedaulatan negara.[2]

Seiring perkembangan zaman dan teknologi digital, motif kejahatan terorisme mengalami transformasi signifikan dengan memanfaatkan internet dan media sosial sebagai sarana utama operasional dalam melakukan perekrutan, kampanye dan penggiringan opini terhadap target yang dituju melalui aplikasi pesan terenkripsi, dan forum daring yang menyebabkan perluasan dari potensi ini menjadi semakin tinggi. Kondisi ini mendorong negara untuk melakukan perluasan kewenangan secara daring salah satunya melalui *cyber surveillance*. *Cyber surveillance* adalah bentuk pengawasan yang dilakukan oleh negara atau otoritas tertentu terhadap aktivitas individu atau kelompok di ruang siber (*cyberspace*) khususnya terhadap komunikasi elektronik, lalu lintas data dan aktivitas digital dengan tujuan tertentu seperti keamanan nasional.[3]

Cyber surveillance yang dilakukan oleh negara hadir sebagai perangkat untuk melakukan pencegahan adanya tindak pidana terorisme yang dilakukan melalui transaksi elektronik dengan adanya upaya untuk melakukan penindakan dan untuk deteksi dini terhadap munculnya dugaan potensi kejahatan. Hal ini sejalan dengan tujuan yang diterapkan oleh adanya perlindungan hukum digital di Indonesia,

---

[1] Indonesia, *Undang-Undang tentang Pemberantasan Tindak Pidana Terorisme*, UU No.5 Tahun 2018, LN Tahun 2003 No.45, TLN No.4284, Ps.1 ayat (2).

[2] Rahmatullah, *Kejahatan Terorisme sebagai Extraordinary Crime dalam Perspektif Hukum Pidana Internasional*, Jurnal Ilmu Hukum Sui Generis, Vol.2, No.1 (Januari 2022), p.48.

[3] David Lyon, *Surveillance Society: Monitoring Everyday Life*, Open University Press, Philadelphia, 2002, p.39.

terutama melalui Undang-Undang ITE. Namun di sisi lain, *cyber surveillance* menimbulkan potensi adanya benturan dengan hak privasi sebagai hak fundamental yang dijamin oleh konstitusi dan instrumen Hak Asasi Manusia (HAM). Hal ini sejalan dengan konsiderans huruf a Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menyebutkan bahwa perlindungan data pribadi dan hak privasi merupakan bagian dari hak asasi manusia yang harus diberi landasan hukum untuk memberikan jaminannya.

Sejumlah penelitian terdahulu menunjukan pentingnya penanganan kejahatan terorisme. Penelitian Rahmatullah menemukan bahwa kejahatan terorisme merupakan kejahatan luar biasa (*extraordinary crime*) yang metode penanganannya pun harus dilakukan secara luar biasa.[4] Penelitian Danang Enggartyasto dan Irwan Hafid menemukan bahwa peraturan tindak pidana terorisme siber yang dimiliki oleh Indonesia saat ini belum begitu komprehensif.[5] Penelitian Ardison Asri menemukan bahwa tindak pidana terorisme siber merupakan pengembangan dari tindak pidana terorisme konvensional.[6] Penelitian Muhammad Luthfi Amirullah menemukan bahwa Indonesia belum memiliki undang-undang atau peraturan khusus yang mengatur *cyber terrorism*.[7]

Berdasarkan kesenjangan itu penelitian ini memiliki kebaruan karena meninjau lebih jauh mengenai aspek-aspek yang perlu diperhatikan dalam membentuk penegakan hukum terhadap cyber terrorism. Penelitian ini melibatkan hak asasi manusia berupa perlindungan privasi yang menjadi objek penelitian dalam upaya harmonisasi pemberlakuan penegakan hukum terhadap *cyber terrorism* yang tidak dibahas pada penelitian-penelitian sebelumnya. Melalui pendekatan normatif, penelitian ini berupaya menemukan keseimbangan antara hak privasi dan keamanan nasional.

---

[4] Rahmatullah, *Op.Cit.*, p.46-54.

[5] Danang Enggartyasto dan Irwan Hafid, *Kebijakan Hukum Pidana terhadap Upaya Pemberantasan Terorisme Siber di Indonesia*, Jurnal Lex Renaissance, Vol.7, No.1 (Januari 2022), p.84-99. https://doi.org/10.20885/JLR.vol7.iss1.art7

[6] Ardison Asri dkk., *Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia*, Jurnal Ilmiah Hukum Dirgantara, Vol.15, No.1 (Desember 2024), p.1-13. https://doi.org/10.35968/jh.v15i1

[7] Muhammad Luthfi Amirullah dkk., *Sistem Pertahanan NKRI dalam Menghadapi Ancaman Cyber Terrorism pada Era Digitalisasi*, Jurnal Al Hakam, Vol.2, No.2 (Oktober 2021), p.82-93. https://doi.org/10.58787/alhakam.v2i2.21

Permasalahan ini hadir melalui pemberlakuan Pasal 31 Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme yang menyatakan penyidik berwenang untuk melakukan penyadapan terhadap adanya dugaan persiapan dan perencanaan tindak pidana terorisme. Kekosongan hukum dari adanya penerapan pasal ini ialah terkait dengan mekanisme pengawasan pasca penyadapan dan perlindungan hasil data yang belum diatur secara komprehensif sehingga menimbulkan adanya potensi pelanggaran hak privasi.[8] Norma ini belum mengatur secara tegas bahwa penyadapan merupakan upaya terakhir. Ketiadaan syarat dan urgensi ini membuka ruang polemik normatif karena dari aspek *necessity* akan menimbulkan adanya penyadapan secara berlebihan.

Berdasarkan uraian latar belakang dan permasalahan tersebut, maka rumusan masalah dari penulisan ini adalah sebagai berikut:

1. Bagaimana pengaturan *cyber surveillance* diterapkan dalam penanganan tindak pidana terorisme sebagai upaya menjaga keamanan nasional?
2. Bagaimana kedudukan hak privasi dalam konteks penerapan *cyber surveillance* menurut hukum nasional dan instrumen hak asasi manusia?
3. Bagaimana model pengaturan *cyber surveillance* yang ideal agar mampu menyeimbangkan kepentingan keamanan nasional dan hak privasi?

B. PEMBAHASAN

1. Pengaturan *Cyber Surveillance* dalam Penanganan Tindak Pidana Terorisme di Indonesia

Upaya penegakan hukum terhadap terorisme siber hingga kini masih bersifat parsial dan tersebar dalam sejumlah peraturan perundang-undangan, khususnya Undang-Undang Nomor 5 Tahun 2018 tentang perubahan atas Undang-Undang Pemberantasan Tindak Pidana Terorisme serta Undang-Undang Nomor 19 Tahun 2016 sebagai perubahan atas Undang-Undang Informasi dan Transaksi Elektronik.[9]

---

[8] Marco Wednesto Larega, *Tinjauan Yuridis Pasal 31 Dan 31a Undang-Undang Republik Indonesia No 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme*, Skripsi, Universitas Brawijaya, Malang, 2019, p.28.

[9] Peter Guntara, *Penegakan Hukum terhadap Tindak Pidana Siber Terorisme di Indonesia*, Jurnal Intelek Insan Cendikia, Vol.2, No.12 (Desember 2025), p.19531.

Kendati demikian, belum terdapat pengaturan khusus yang secara tegas dan komprehensif mengklasifikasikan terorisme siber sebagai satu bentuk tindak pidana yang berdiri sendiri. Kondisi tersebut menimbulkan kekosongan norma, karena ketentuan yang ada umumnya hanya dimanfaatkan untuk menjerat perbuatan yang berkaitan atau mendukung aktivitas terorisme, tanpa mampu mengakomodasi secara utuh dan sistematis kompleksitas kejahatan terorisme siber.[10]

Selain itu hingga saat ini belum terdapat pengaturan secara khusus terkait *cyber terrorism*. Dalam kondisi kekosongan pengaturan tersebut, Asean Convention on Counter Terrorism serta International Convention for the Supression of Terrorist Bombings dapat dijadikan landasan hukum untuk menjerat pelaku *cyber terrorism*. Indonesia sendiri telah mengesahkan kedua konvensi tersebut, yaitu Asean Convention on Counter Terrorism melalui Undang-Undang Nomor 5 Tahun 2012 tentang pengesahannya, sementara International Convention for the Supression of Terrorist Bombings diratifikasi melalui Undang-Undang Nomor 5 Tahun 2006 tentang pengesahannya.[11]

Secara garis besar, pendekatan penegakan hukum terhadap tindak pidana *cyber terrorism* di Indonesia dilihat melalui adanya kebijakan integral berbasis *penal* dan *non penal* yang kemudian mewujudkan adanya positifisasi dan kriminalisasi perbuatan tindak pidana terorisme.[12] Pedoman pelaksanaan dari penegakan hukum ini tentunya tunduk pada sumber hukum pidana di Indonesia seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) sebagai pedoman utama pelaksanaan teknisnya.

Aksi teror melalui dunia maya telah banyak terjadi di berbagai negara termasuk Indonesia. Kasus yang terjadi pada kedutaan Sri Lanka di berbagai negara yang dibanjiri oleh hampir 800 email yang semuanya berisi tentang ancaman dari kelompok yang menamakan dirinya *Black Tigers*. Begitu pula *cyber terrorism* terjadi di Eropa yang dilakukan oleh Greek Security and Intrude dimana serangan dilakukan terhadap sistem komputer European Organization For Nuclear Research

[10] *Ibid*.
[11] Alfira N. Samad, *Analisis Instrumen Cyber Terrorism dalam Kerangka Sistem Hukum Internasional*, Skripsi, Universitas Hassanudin, Makassar, 2014, p.4. http://repository.unhas.ac.id/handle/123456789/10123
[12] Ardison Asri dkk., *Op.Cit.*, p. 8.

(pengembangan nuklir terbesar di dunia). Di tahun 2016 muncul serangan *virus ransomware wannacry* terhadap beberapa rumah sakit di hampir 100 negara di seluruh dunia, termasuk Indonesia.[13]

Dalam konteks keamanan nasional, keberadaan intelijen sebagai garda terdepan dalam deteksi dan antisipasi ancaman memiliki peranan yang sangat strategis, khususnya dalam menghadapi tindak pidana terorisme yang bersifat laten, terorganisir, dan berjejaring lintas wilayah. Kepolisian Republik Indonesia melalui fungsi intelkam, memiliki mandat untuk melakukan pengumpulan, pengolahan, dan analisis informasi terkait potensi gangguan keamanan termasuk aktivitas yang mengarah pada radikalisme dan terorisme.[14]

Pada aspek penindakan, strategi yang dijalankan menunjukan keberhasilan yang signifikan dalam mengungkap jaringan terorisme. Penangkapan individu yang terlibat baik pelaku utama, pendukung logistik, maupun simpatisan, mencerminkan kemampuan Intelkam dalam mendeteksi aktivitas terorisme. Penindakan ini diperkuat dengan penggunaan teknologi pengawasan modern, seperti analisis media sosial untuk melacak propaganda digital. Namun salah satu kelemahan utama dari strategi penindakan adalah minimnya pendekatan rehabilitatif untuk para pelaku yang telah ditangkap.[15]

Selain itu, Indonesia juga memiliki lembaga yang bertanggungjawab dalam keamanan *cyberspace* nasional yaitu Badan Siber dan Sandi Negara (BSSN) sebagai lembaga utama yang atas koordinasi lintas sektor dalam pengelolaan insiden siber, pengembangan sistem keamanan digital nasional, serta penyusunan kebijakan dan pedoman teknis yang menjadi acuan bagi kementerian, lembaga, serta sektor swasta.[16]

Maka dari itu, dapat dilihat bahwa pengaturan terhadap *cyber terrorism* di Indonesia tidak sepenuhnya mengalami kekosongan, melainkan belum diatur secara harmonis dan sistematis yang menyebabkan masih banyaknya celah terhadap tindak pidana terorisme berbasis siber.

---

[13] Ardison Asri dkk., *Op.Cit.*, p.2.

[14] Suman Sirait, *Peran Intelijen Keamanan dalam Pencegahan dan Penanggulangan Tindak Pidana Terorisme*, Jurnal USM Law Review, Vol.8, No.2 (Mei 2025), p.677.

[15] *Ibid*..

[16] Galang Ramadhan, *Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber*, Jurnal Hukum Administrasi Publik dan Ilmu Komunikasi, Vol.2, No.2 (2025), p.4.

2. Kedudukan Hak Privasi dalam Konteks Penerapan *Cyber Surveillance*

Pengaturan tentang aktivitas elektronik di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan tujuan pembentukannya adalah untuk melindungi dan memberikan kepastian hukum bagi masyarakat yang melakukan transaksi elektronik, mencegah terjadinya kejahatan berbasis teknologi informasi dan komunikasi, serta melindungi masyarakat pengguna jasa yang memanfaatkan transaksi elektronik.[17] Pemberlakuan undang-undang ini merupakan bentuk kriminalisasi terhadap praktik kejahatan di ruang siber termasuk pelanggaran hak privasi.

Di Indonesia kesadaran akan perlunya perlindungan data pribadi semakin meningkat, terutama seiring dengan pertumbuhan jumlah pengguna internet dan aplikasi berbasis teknologi lainnya. Berdasarkan Pasal 28G ayat (1) UUD 1945, warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta miliknya. Dalam perkembangan teknologi yang pesat saat ini, hak privasi harus pula diartikan sebagai hak pribadi yang perlu untuk dilindungi karena sifatnya yang sensitif dan melekat pada diri individu.

Apabila perlindungan data dipandang sebagai salah satu unsur dalam relevansi pengawasan (*surveillance*) berbasis hak asasi manusia, maka unsur lainnya adalah penekanan pada hak individu untuk menjalani kehidupan yang bebas dari pengamatan dan campur tangan yang tidak diinginkan. Hak atas privasi pada hakikatnya merupakan hak yang bersifat relatif. Hal ini karena negara juga memiliki kewajiban untuk memprioritaskan kepentingan keamanan nasional melalui pencegahan dan penegakan hukum terhadap kejahatan, perlindungan terhadap kesehatan publik dan keselamatan pihak secara menyeluruh.[18]

Hukum berperan sebagai instrumen untuk merumuskan batasan mengenai waktu, cara, subjek serta pihak yang menjadi objek pembatasan hak privasi. Setiap pelanggaran atas kepercayaan atau kerahasiaan dapat menimbulkan konsekuensi hukum berupa pemberian kompensasi setelahsuatu peristiwa terjadi, khususnya di dalam situasi dimana pengawasan dan pendistribusian dilakukan secara tidak sah.[19]

---

[17] Sahat Maruli T. Situmeang, *Cyber Law*, CV. Cakra, Bandung, 2020, p.18.
[18] Gary T. Marx, *Routledge Handbook of Surveillance Studies*, Routledge, New York, 1998.
[19] Anggi Anggraeni Kusumoningtyas, *Dilema Perlindungan Data Pribadi dan Pengawasan Siber: Tantangan di Masa Depan*, Jurnal Legislasi Indonesia, Vol.17, No.2 (Juni 2020), p.240.

Hal ini perlu sejalan dengan asas proporsionalitas yang menuntut agar pembatasan hak pribadi melalui pengawasan siber memiliki hal-hal berikut[20]:

a. Tujuan yang sah seperti keamanan nasional melalui pencegahan terorisme
b. Kesesuaian untuk mencapai tujuan tersebut
c. Bersifat mendesak artinya tidak ada alternatif lain yang lebih ringan untuk dapat dilakukan
d. Keseimbangan antara manfaat keamanan dan kerugian terhadap hak privasi

Asas ini sangat relevan karena pengawasan siber merupakan bentuk pembatasan hak konstitusional yang tidak boleh dilakukan secara berlebihan. Pembatasan ini dapat dilihat melalui Putusan Mahkamah Konstitusi RI No. 5/PUU-VIII/2010 yang menyatakan bahwa penyadapan adalah pembatasan HAM yang dapat dibenarkan untuk kepentingan nasional namun harus diatur dengan Undang-Undang dan ketentuan yang jelas untuk memastikan legalitas dan transparansi pemberlakuannya.[21]

Dalam poin pertimbangan Hakim Mahkamah Konstitusi di putusan tersebut dijelaskan bahwa hak privasi bukanlah bagian dari hak-hak yang tidak dapat dikurangi dalam keadaan apapun (*non derogable rights*), sehingga negara dapat melakukan pembatasan terhadap pelaksanaan hak-hak tersebut dengan menggunakan Undang-Undang, sebagaimana diatur dalam Pasal 28J ayat (2) Undana-Undang Dasar Negara Republik Indonesia Tahun 1945.[22]

Disamping itu, Hakim Mahkamah Konstitusi menjelaskan bahwa tata cara penyadapan atau intersepsi harus diatur dalam dengan hukum acara pidana atau undang-undang penyadapan tersendiri guna mencegah adanya potensi pelanggaran privasi dan pelanggaran kepastian hukum. Hal ini yang masih menjadi aspek kekosongan hukum di Indonesia mengingat pengaturannya belum memadai secara komprehensif.

---

[20] Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, Ps.28J ayat (2).

[21] Indonesia, *Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Terhadap Undang-Undang Dasar 1945*, Putusan Mahkamah Konstitusi No.5/PUU-VIII/2010, p.16. https://www.mkri.id/putusan/putusan_sidang_Putusan_5_PUU_VIII_2010.pdf

[22] *Ibid*., p.11.

Pembatasan hak privasi dalam rangka menjaga keamanan nasional, khususnya untuk mencegah dan menangani potensi tindak pidana terorisme digital, merupakan langkah yang secara hukum dapat dibenarkan sepanjang memenuhi prinsip-prinsip negara hukum dan penghormatan terhadap hak asasi manusia. Tantangan utama ke depan adalah memastikan terciptanya keseimbangan yang berkelanjutan antara kebutuhan akan keamanan nasional dan perlindungan hak privasi warga negara, sehingga upaya penanggulangan terorisme digital tidak hanya efektif secara operasional, tetapi juga sah secara hukum dan legitim secara demokratis.

3. Model Pengaturan *Cyber Surveillance* yang Ideal dalam Menyeimbangkan Keamanan Nasional dan Hak Privasi

Model pengaturan *cyber surveillance* yang ideal dalam menyeimbangkan keamanan nasional dan hak privasi dapat diwujudkan melalui kerangka hukum yang jelas seperti UU PDP khususnya dalam Bab 4 Pasal 5 sampai 15 yang menjelaskan mengenai hak subjek data pribadi, pengawasan independen, pembatasan akses terhadap data secara spesifik dengan adanya persetujuan, penerapan prinsip minimalisasi data, transparansi dan akuntabilitas lembaga pelaksana serta teknologi enkripsi kuat, memastikan pengawasan hanya sebagai upaya terakhir.

Penguatan kapasitas teknologi dan pembangunan infrastruktur menjadi elemen penting dalam strategi nasional di bidang keamanan siber. Salah satu bentuk implementasinya adalah penerapan sistem *honeypot* berbasis otomasi yang berfungsi untuk mengidentifikasi serta menganalisis aktivitas siber yang mencurigakan secara langsung (*real-time*). Pemanfaatan teknologi kecerdasan buatan (*artificial intelligence*) dan *machine learning* mulai dikembangkan guna meningkatkan kemampuan deteksi dini terhadap potensi serangan terorisme berbasis siber.[23]

Di samping itu, perlu dipahami keamanan siber tidak semata-mata hanya menjadi tanggungjawab pemerintah. Keterlibatan sektor swasta dan masyarakat juga memiliki peran krusial dalam membangun ketahanan digital nasional yang berkelanjutan. Pada konteks tersebut, pendekatan *Public Private Partnership* (PPP)

[23] Galang Ramadhan, *Op.Cit.*, p. 264.

dipandang sebagai strategi yang efektif karena memungkinkan kolaborasi lintas sektor dalam penerapan sistem manajemen keamanan informasi (*Information Security Management System*/ISMS) serta pembentukan mekanisme respons insiden yang terpadu, efisien dan terkoordinasi.[24]

Pada dasarnya seluruh konsep ini dapat diharmonisasikan dengan memperhatikan asas universalitas dalam hukum siber. Asas ini patut mendapatkan perhatian khusus dalam konteks penanganan hukum terhadap berbagai kejahatan siber. Asas tersebut dikenal juga dengan istilah universal interest jurisdiction. Seiring berjalannya waktu, cakupan penerapan asas ini mengalami perluasan hingga meliputi kejahatan-kejahatan berat terhadap kemanusiaan (*crimes against humanity*), seperti penyiksaan, genosida, pembajakan pesawat udara, dan bentuk kejahatan serius lainnya.[25]

Kedepannya tidak tertutup kemungkinan bahwa prinsip jurisdiksi universal ini juga akan dikembangkan untuk menjangkau tindak pidana di ruang siber, seperti pembajakan digital, peretasan sistem komputer, *carding*, *cracking*, serta penyebaran virus. Namun demikian, perlu ditegaskan bahwa penerapan asas ini seharusnya dibatasi hanya pada kejahatan-kejahatan yang memiliki tingkat keseriusan tinggi, sebagaimana diakui dalam perkembangan hukum internasional seperti kejahatan terorisme itu sendiri. Oleh karena itu, penanganan kejahatan di ruang siber menuntut adanya pembentukan kerangka hukum baru yang tidak semata-mata bertumpu pada batas-batas teritorial negara.

Kondisi ini mencerminkan pergeseran paradigma penanganan keamanan siber, dari pendekatan yang bersifat reaktif menuju preventif, di mana sistem mampu mengenali pola ancaman sebelum menimbulkan dampak yang lebih luas terhadap infrastruktur strategis negara. Pemerintah ingin memastikan bahwa keamanan dan kenyamanan mereka dalam melakukan akses dan transaksi elektronik dapat dilakukan dengan baik.

C. PENUTUP

Berdasarkan hasil pembahasan, ditemukan bahwa terdapat kesenjangan antara wewenang negara dalam menerapkan pengawasan siber untuk mencegah

[24] *Ibid*.
[25] Sahat Maruli T. Situmeang, *Op.Cit*., p.13.

upaya terorisme digital dengan potensi pelanggaran hak privasi yang merupakan suatu hak asasi manusia yang melekat bagi seluruh individu. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik memberikan pengaturan mengenai perlindungan seluruh individu dalam mengakses ruang siber termasuk hak privasi.

Hal ini diselaraskan dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang secara khusus dan spesifik mengatur mengenai bentuk-bentuk perlindungan data pribadi yang harus dijamin oleh pemerintah secara menyeluruh. Pelanggaran privasi dapat terjadi apabila terdapat suatu oknum maupun pihak yang dianggap merugikan suatu individu dalam mengakses informasi atau data pribadi yang bersifat *confidential* sehingga menjadi tantangan tersendiri.

Namun pada dasarnya hak privasi merupakan suatu hak yang dapat dibatasi oleh hukum apabila diterapkan sesuai dengan urgensi dan kebermanfaatan kolektif seperti keamanan nasional dari ancaman terorisme digital. Hal ini diperkuat oleh pernyataan Pasal 28J ayat (2) UUD RI 1945 dan Putusan Mahkamah Konstitusi RI No. 5/PUU-VIII/2010 yang menyatakan bahwa hak privasi dapat dibatasi oleh hukum dalam keadaan tertentu.

Sebaiknya pemerintah menyusun regulasi yang komprehensif terkait dengan pertanggungjawaban pasca penyadapan untuk menjamin transparansi kegunaan dari tindakan siber yang mereka lakukan. Hal ini dapat diwujudkan melalui reformasi Undang-Undang di sektor siber dan penyusunan peraturan khusus mengenai pencegahan tindak pidana dan kejahatan berbasis teknologi siber yang memungkinkan pemerintah dan masyarakat sama-sama memahami konsekuensi dan kewajiban hukum antara keduanya.

DAFTAR PUSTAKA

Buku

Lyon, David. 2002. *Surveillance Society:Monitoring Everyday Life*. (Philadelphia: Open University Press).

Marx, Gary T.. 1998. *Routledge Handbook of Surveillance Studies*. (New York: Routledge).

Situmeang, Sahat Maruli T.. 2020. *Cyber Law*. (Bandung: CV. Cakra).

Publikasi

Amirullah, Muhammad Luthfi dkk. *Sistem Pertahanan NKRI dalam Menghadapi Ancaman Cyber Terrorism pada Era Digitalisasi*. Jurnal Al Hakam. Vol.2. No.2 (2021).

Asri, Ardison dkk. *Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia*. Jurnal Ilmiah Hukum Dirgantara. Vol.15. No.1 (Desember 2024).

Enggartyasto, Danang dan Irwan Hafid. *Kebijakan Hukum Pidana terhadap Upaya Pemberantasan Terorisme Siber di Indonesia*. Jurnal Lex Renaissance. Vol.7. No.1 (Januari 2022).

Guntara, Peter. *Penegakan Hukum terhadap Tindak Pidana Siber Terorisme di Indonesia*. Jurnal Intelek Insan Cendikia. Vol.2. No.12 (Desember 2025).

Kusumoningtyas, Anggi Anggraeni. *Dilema Perlindungan Data Pribadi dan Pengawasan Siber: Tantangan di Masa Depan*. Jurnal Legislasi Indonesia. Vol.17. No.2 (Juni 2020).

Rahmatullah. *Kejahatan Terorisme sebagai Extraordinary Crime dalam Perspektif Hukum Pidana Internasional*. Jurnal Ilmu Hukum Sui Generis. Vol.2. No.1 (Januari 2022).

Ramadhan, Galang. *Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber*. Jurnal Hukum Administrasi Publik dan Ilmu Komunikasi. Vol.2. No.2 (2025).

Sirait, Suman. *Peran Intelijen Keamanan dalam Pencegahan dan Penanggulangan Tindak Pidana Terorisme*. Jurnal USM Law Review. Vol.8. No.2 (Mei 2025).

Karya Ilmiah

Larega, Marco Wednesto. 2019. *Tinjauan Yuridis Pasal 31 dan 31a Undang-Undang Republik Indonesia No 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme*. Skripsi. Malang: Universitas Brawijaya.

Samad, Alfira Nurliliani. 2014. *Analisis Instrumen Cyber Terrorism dalam Kerangka Sistem Hukum Internasional*. Skripsi. Makassar: Universitas Hassanudin.

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 92. Tambahan Lembaran Negara Republik Indonesia Nomor 6216.

Putusan Mahkamah Konstitusi Republik Indonesia Nomor 5/PUU-VIII/2010.