Jurnal Ilmu Hukum "THE JURIS" Vol. IX, No. 2, Desember 2025
ISSN 2580-0299, e-ISSN 2580-8370
http://ejournal.stih-awanglong.ac.id/index.php/juris

PERLINDUNGAN HUKUM DI RUANG SIBER: TELAAH YURIDIS ATAS RANCANGAN UNDANG-UNDANG KEAMANAN DAN KETAHANAN SIBER

Suharto[1*], Dian Eka Kusuma Wardani[2], Ali Rahman[3], Muhammad Irwan[4]
[1,2,3]Universitas Sawerigading Makassar, Makassar, Indonesia
[4]Universitas Hasanuddin makassar, Makassar, Indonesia
attobareto96@gmail.com[1*], dianunsa@gmail.com[2], alirahmann1990@gmail.com[3],
muhammad.irwan@unhas.ac.id[4]

Abstract

This study aims to analyze the legal framework of the Draft Law on Cybersecurity and Resilience (RUU KKS) in ensuring the protection of national strategic infrastructure and data, as well as to identify potential legal issues that may arise. The background of this research is driven by the growing threats of cybercrime in Indonesia, which have significant implications for national security, economic stability, and the protection of personal data. The research method employed is normative legal research using a conceptual approach and a statute approach. The data were collected from laws and regulations, academic literature, and relevant court decisions. The analysis technique used is qualitative descriptive, interpreting legal principles and assessing the coherence of existing regulations with the needs of national cybersecurity protection. The findings indicate that Indonesia's current cybersecurity regulations remain fragmented across several sectoral laws, resulting in overlaps and weaknesses in ensuring legal certainty. The RUU KKS is expected to serve as a comprehensive legal instrument that strengthens the protection of critical infrastructure, prevents cyber misuse, and balances state interests with the protection of individual rights. Anchored in Pancasila and the 1945 Constitution, this regulation is essential to reinforce Indonesia's digital sovereignty

Keywords: *Cybersecurity, Draft Law on Cybersecurity and Resilience, Legal Protection*

✉ Alamat korespondensi:
Universitas Sawerigading Makassar, Makassar, Indonesia
attobareto96@gmail.com

I. PENDAHULUAN

Secara filosofis, melekat dua fungsi pada negara sebagai suatu unit politik, yaitu fungsi keamanan dan fungsi kesejahteraan. Fungsi keamanan yang melekat pada negara tersebut kemudian melahirkan istilah keamanan nasional. Jika dilihat dari tujuannya, keamanan nasional dimaksudkan untuk melindungi negara dari berbagai ancaman yang dapat meruntuhkan negara. Dalam kerangka statis, keamanan nasional biasanya selalu menyangkut tentang aktor, tanggung jawab untuk menyelenggarakan keamanan nasional selalu dilekatkan pada Negara (Widjajanto dkk., 2013).

Keamanan nasional termasuk juga dalam meminimalisir bahaya dan ancaman. Ancaman dapat dilihat sebagai antisipasi terhadap penghalang dari beberapa nilai-nilai. Ketika berbicara mengenai perlindungan maka biasanya terkait dengan bebas dari penghalang dan rintangan dari apa yang dinikmati sebagai hasil yang bernilai. Keamanan nasional akhirnya berujung menjadi kepentingan nasional dengan mengacu pada hasil bernilai yang diinginkan oleh mereka yang berada dalam basis efektif politik suatu bangsa, sehingga nilai yang ada tersebut biasanya diasosiasikan dengan konsep kepentingan nasional. Konsep keamanan nasional akan terus berkembang dan berubah, terutama pada hasil nilai yang diinginkan, lingkungan internasional, kondisi domestik, sifat ancaman, dan strategi menghadapi ancaman (Lasswell, 1950).

Secara rinci, konsep keamanan manusia dapat dilihat dalam tujuh komponen yang harus mendapatkan perhatian yaitu, 1) *economic security* (bebas dari kemiskinan dan jaminan pemenuhan kebutuhan hidup, 2) *food security* (kemudahan akses terhadap kebutuhan pangan), 3) *health security* (kemudahan mendapatkan layanan kesehatan dan proteksi dari penyakit), 4) *environmental security* (proteksi dari polusi udara dan pencemaran lingkungan, serta akses terhadap air dan udara bersih), 5) *personal security* (keselamatan dari ancaman fisik yang diakibatkan oleh perang, kekerasan domestik, kriminalitas, penggunaan obat-obatan terlarang, dan bahkan kecelakaan lalu lintas), 6) *community security* (kelestarian identitas kultural dan tradisi budaya), dan 7) *political security* (perlindungan terhadap hak asasi manusia dan kebebasan dari tekanan politik). Tujuh komponen diatas bisa disimplifikasi menjadi dua komponen utama, yaitu freedom from fear (bebas dari rasa takut) dan freedom from want (bebas dari ketidakmampuan untuk memiliki) (Fitrah, 2015).

Keamanan siber menjadi subsistem dari keamanan nasional. Seperti yang disebutkan oleh Paleri misalnya *cyber security* muncul menjadi salah satu bagian dari keamanan nasional. Ditambah lagi bila digabungkan dengan konsep baru keamanan manusia, perhatian atas konsep keamanan manusia, personal security memiliki keterkaitan erat dengan Keamanan Siber. Ringkasnya menurut penulis komponen dari keamanan nasional yang perlu mendapatkan perhatian sebagai upaya perlindungan kepada negara dan bangsa yaitu 1) sumber daya manusia, termasuk pada militer dan aparat terkait serta masing-masing warga negara, 2) teknologi, yaitu baik infrastruktur yang mendukung kehidupan masyarakat maupun perangkat-perangkat teknologi dalam upaya memberikan perlindungan pada keamanan nasional, dan juga 3) hukum atau norma yang mengatur tentang perlindungan terkait keamanan. Komponen teknologi menjadi dasar untuk melihat kepentingan Keamanan Siber dalam upaya perlindungan keamanan nasional (Buzan & Hansen, 2009).

Kejahatan siber (*cybercrime*) sebagai kategori tindak pidana modern memiliki karakteristik unik yang membedakannya dari kejahatan konvensional (Cahyono dkk., 2025). Beberapa tahun terakhir, ancaman terhadap keamanan siber di Indonesia semakin meningkat, baik dalam skala individu, perusahaan, maupun negara. Serangan siber seperti peretasan (*hacking*), penyebaran *Malware* dan *Ransomware* seperti yang belum lama ini terjadi di Pusat Data Sementara Nasional (PDSN) di Surabaya, dan serangan *denial-of-service* (DoS) menjadi isu yang sangat serius dan dapat merugikan berbagai sektor, termasuk sektor pemerintahan, ekonomi, hingga sektor kritis seperti energi dan infrastruktur. Studi yang dilakukan oleh Indonesia Cyber Security Forum (ICSF) menunjukkan bahwa sekitar 60% perusahaan di Indonesia belum memiliki kebijakan keamanan data yang memadai (Sihotang dkk., 2025), Oleh karena itu, perlindungan terhadap ruang siber menjadi salah satu prioritas utama dalam kebijakan nasional banyak negara di dunia.

Untuk mencegah kejahatan sibers, individu dan pemerintah perlu memahami dengan jelas skema kejahatan di dunia maya dan tren serta perilaku Internet kontemporer dan berkelanjutan dari para penjahat ini. Saat ini, pencurian kartu kredit dan kasus pencucian uang online kejahatan dunia maya semakin meningkat. Pelecehan dan pencemaran nama baik melalui media sosial juga menjadi perhatian individu (Butarbutar, 2023). Lebih lanjut, dalam ranah pelanggaran *privacy*, akan muncul

pertanyaan, bagaimana kepastian hukum untuk melindungi privasi seseorang termasuk data pribadinya (Felzmann dkk., 2019).

Terkait dengan landasan yuridis dalam undang-undangan keamanan siber, sesuai dengan ketentuan yang ada dalam Pasal 10 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan, kemudian harus dilihat pada materi muatan yang harus diatur dalam undang-undang berisi mengenai, pengaturan lebih lanjut mengenai ketentuan UUD 1945, perintah suatu undang-undang untuk diatur dengan undang-undang, serta pemenuhan kebutuhan hukum dalam masyarakat. Peratuan perundang-undangan ini digunakan sebagai acuan dalam pembuatan suatu peraturan perundang-undangan lainnya, dengan adanya hukum siber yang tegas di dunia internasional, diharapkan mampu meredam maraknya kejahatan di dunia siber. Sebelum hal tersebut terlaksana, alangkah lebih bijaknya jika Indonesia menata kembali penguasaan teknologi dan membuat undang-undang khusus terkait ancaman siber selain di darat, laut, udara, dan ruang angkasa (Manurung, 2024).

Berdasarkan uraian tersebut diatas penulis mengangkat isu dalam penelitian ini berupa pengaturan hukum dalam RUU keamanan dan ketahanan siber dalam menjamin perlindungan terhadap infrasturktur dan data strategis nasional di ruang siber dan mengurai potensi permasalahan yuridis yang dapat muncul dalam RUU keamanan dan ketahanan siber.

II. METODE PENELITIAN

Penelitian ini merupakan penelitian tipe normatif yang bersifat deskriptif (Amiruddin, 2016), dengan menggunakan Pendekatan Penelitian ini adalan konseptual (*conseptual approach*) dan Pendekatan PerUndang-Undangan (*Statute Approach)* yang dilakukan dengan cara menelaah semua Undang-Undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang diteliti (Irwansyah, 2020). Pengolahan dan analisis bahan hukum dan penelitian ini menggunakan metode penelitian kualitatif dengan mengumpulkan dan menemukan bahan hukum yang berupa PerUndang-Undangan, literatur-literatur/buku-buku, dan Putusan Pengadilan yang kemudian dianalisis. Hasil analisis itu dapat berupa penggambaran atau deskripsi. Dari bahan hukum itu, peneliti membuat interpretasi dan penilaian untuk menangkap korespondensi dan koherensi yang ada dalam bahan hukum dengan menggunakan beberapa Perspektif Asas/Prinsip Hukum.

III. HASIL DAN PEMBAHASAN

Media elektronik tidak dapat disangkal memang memfasilitasi aktivitas masyarakat global dan salah satunya dalam transaksi bisnis, terutama bisnis keuangan di samping bisnis lainnya. Bertepatan dengan kemajuan teknologi dan informasi publik dibuat untuk mengikuti semua perkembangan yang terjadi. sedang terjadi (Sugiartha dkk., 2021). Dalam berkomunikasi dan bersosialisasi sangat diperlukan kemajuan teknologi dan informasi, karena hal tersebut memudahkan masyarakat dalam segala hal, yaitu berkomunikasi dengan cara baru, berjualan dengan cara baru, dan berbisnis tanpa batasan waktu dan tempat (Sakban dkk., 2020). Hal ini membuka mata masyarakat dengan dunia baru yang perkembangannya sangat pesat. Internet merupakan salah satu metode yang sangat sering digunakan dalam hal ini karena internet merupakan salah satu perkembangan teknologi yang telah mengubah dunia dari tahun ke tahun (Damayanti & Ismowati, 2021).

Cybercrime ialah frasa yang dapat digunakan dalam mendeskripsikan kegiatan kejahatan yang menjadikan jaringan komputer/komputer sebagai tempat kejadian, sasaran, maupun alat kejahatan. Di antara peristiwa yangdapat dikategorikan sebagai cybercrime antara lain ialah penipuan identitas, carding/penipuan kartu, penipuan lelang secara daring, pornografi anak, confidence fraud, serta pemalsuan cek (Halim & Prasetyo, 2018). menyatakan bahwasanya cybercrime ialah perkembangan bentuk kejahatan yang terjadi pada real space, adapun cyber warfareialah perkembangan dari bentuk perang yang terjadi pada *real space*. Selanjutnya, *cyber attack* didefinisikan secara berbeda dari kedua istilah sebelumnya.

Cybercrime yang dilakukan dengan cara menyusup ke sistem jaringan komputer secara ilegal, tanpa izin atau sepengetahuan pemilik sistem jaringan komputerdimasukkan Biasanya, pelaku (cracker) menyabotase atau mencuri informasi berharga dan rahasia. Namun, ada pula yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus sistem yang

memiliki tingkat proteksi tinggi (Santhi & Nuarta, 2023). Serang siber merupakan bentuk ancaman kontemporer yang dapat menggangu stabilitas nasional dari berbagai aspek, seperti politik, ekonomi, serta pertahanan dan keamanan negara. Oleh karena itu, penting bagi negara dituntut untuk membangun sistem pertahanan digital yang kuat dan terstruktur. Adanya regulasi dan Undang – Undang Informasi dan Transaksi Elektronik (UU ITE) serta pembentukan lembaga nasional yakni Badan Siber dan Sandi Negara (BSSN) merupakan bentuk afirmasi dan langkah pemerintah Indonesia dalam menjaga kedaulatan digital tersebut (Saputri dkk., 2020).

Secara umum, strategi keamanan siber nasional dirancang dengan mengacu pada kerangka manajemen risiko, yaitu pendekatan terstruktur untuk mengidentifikasi, meganalisis, dan mengurangirisiko yang timbul d iruang siber. Pendekatan ini menyoroti pentingnya pemahaman terhadap ancaman (*threats*), kelemahan sistem (*vulnerabilities*), serta kemungkinan dampak (*impact*) yang dapat ditimbulkan oleh setiap insiden yang terjadi. Strategi ini terdiri dari sejumlah elemen kunci, di antaranya, Dasar hukum dan kebijakan nasional, Lembaga dan sinergi antar sektor, Pelatihan dan literasi keamanan digital, Kerja sama internasional, Infrastruktur nasional untuk keamanan digital Terdiri atas mekanisme pemantauan, sistem deteksi awal, forensik siber, dan pusat komando penanganan insiden (Maharani & Atman, 2025).

Indonesia telah memiliki hukum berupa undang-undang yang secara khusus mengatur mengenai kejahatan dunia maya, yakni Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE). Namun, keseluruhan UU sektoral tersebut tidak mengatur definisi data pribadi. Pengaturan definisi data pribadi dalam peraturan sektoral di bawah UU berdampak pada pemaknaan data pribadi yang berbeda-beda sesuai kebutuhan sektoral dan berpotensi adanya tumpang tindih pengaturan. Dari sisi kekuatan mengikatnya, relatif rendah dibandingkan jika diatur dalam UU, Pada akhirnya kelemahan tersebut akan berpengaruh pada minimnya kepastian hukum. Serupa dengan keberadaan perlindungan data pribadi, dalam konteks keamanan siber, sampai saat ini belum ada regulasi yang khusus mengatur keamanan dan ketahanan siber secara komprehensif. Pengaturan siber nasional masih tersebar dalam berbagai regulasi, antara lain UU Telekomunikasi dan UU ITE (Rongiyati, 2021).

Ruang lingkup pengaturan RUU KKS lebih kepada bagaimana negara beru berupaya untuk mampu melaksanakan keamanan dan ketahanan, dan perlindungan siber di Indonesia, seperti melakukan deteksi, identifikasi, proteksi, penanggulangan, pemulihan, pemantauan, serta pengendalian pada objek-objek keamanan siber. RUU ini penting untuk segera disahkan untuk mengantisipasi dan memitigasi resiko keamanan siber agar kepentingan nasional Indonesia tetap terjaga senantiasa terlindungi. Berbagai macam kasus yang telah disebutkan setidaknya sudah menjadi desakan untuk segera dapat memiliki aturan ketahanan siber yang mumpuni menjaga kedaulatan digital Indonesia (Arief, 2022).

Pemerintah telah mendorong penggunaan teknologi *open source* sebagai bentuk pengurangan ketergantungan terhadap teknologi asing. Pembentukan Angkatan Siber TNI dan penyusunan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) juga mencerminkan keseriusan dalam membangun kapasitas pertahanan siber nasional (Jamil & Agussalim, 2025).

Perumusan peraturan perundang-undangan berfungsi sebagai mekanisme penting untuk memajukan tujuan pembangunan dan merupakan komponen mendasar dari kerangka negara hukum, serta upaya untuk mencapai aspirasi nasional (Saputra & Rahman, 2024). Pada pembentukan suatu peraturan peruundang-undangan juga akan dilihat pada asas-asas dalam suatu RUU, Terhadap Asas yang ada pada RUU Keamanan dan Ketahanan Siber melandasi penyelenggaraan Keamanan Siber dalam upaya-upaya baik pencegahan, penanggulangan, hingga pemulihan dari insiden siber atau serangan siber. Secara filosofis, melekat dua fungsi pada negara sebagai suatu unit politik, yaitu fungsi keamanan dan fungsi kesejahteraan. Fungsi keamanan yang melekat pada negara tersebut kemudian melahirkan istilah keamanan nasional. Jika dilihat dari tujuannya, keamanan nasional dimaksudkan untuk melindungi negara dari berbagai ancaman yang dapat meruntuhkan negara. Dalam kerangka statis, keamanan nasional biasanya selalu menyangkut tentang aktor, tanggung jawab untuk menyelenggarakan keamanan nasional selalu dilekatkan pada negara.

Sehingga dilihat pada Pasal 6 ayat (2) Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan menyatakan bahwa selain mencerminkan asas materi muatan, peraturan

perundang-undangan tertentu dapat berisi asas lain yang sesuai dengan bidang hukum perundangundangan yang bersangkutan, Sehingga bila terjadi suatu insiden yang mengancam keamanan siber maka upaya-upaya perlindungan yang perlu diambil harus mencerminkan keseluruhan asas seperti, Asas keterpercayaan, Asas kesiagaan, dan Asas kolaborati

Terkait dengan Materi muatan yang dapat diatur dalam RUU siber dalam konteks pertahanan dan keamanan negara berupa,

1) Data protection,
2) Cyber security Konsep kemanan siber melingkupi aspek:
   a) Privacy/Confidentiality: Aspek terkait jaminan kerahasiaan isi dari informasi.
   b) Authentication: Aspek yang menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses/memberikan informasi adalah betul-betul orang yang dimaksud.
   c) Integrity: Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
   d) Accesibility: Aspek ini berhubungan denganketersediaan informasi ketika dibutuhkan.
   e) Access control: Aspek ini berhubungan dengan cara pengaturan akses kepadainformasi
   f) Non repudiation.
3) Critical Information Infrastructure,
4) Penyadapan
5) Cyber terorisme
6) E-government
7) Ketentuan pidana dan penegakan hukum.

Selain konteks pertahanan dan keamanan negara, materi muatan yang diperlukan dalam RUU Siber setidaknya antara lain, Aspek Ekonomi, Aspek Ideologi, Aspek Ideologi. Di era informasi dan sosial media berbasis internet, keamanan siber sangat terkait erat dengan stabilitas ideologi, politik, ekonomi, sosial, budaya, pertahanan, dan keamanan, dan bahkan kedaulatan negara. Keamanan siber di Indonesia dipengaruhi oleh dua faktor utama, yakni infrastruktur dan teknologi yang memiliki kesadaran bahwa keamanan dunia siber adalah permasalahan penting terkait dengan pertanahan negara.

Sebuah undang-undang yang baik harus mengandung norma hukum yang diidealkan oleh masyarakat yang menuntun kepada cita-cita luhur kehidupan bermasyarakat dan bernegara. Cita-cita luhur dapat menjadi landasan filosofis yang muncul dalam suatu peraturan perundang-undangan Hal ini memunculkan bahwa landasan filosofis yang ada dalam suatu peraturan perundang-undangan bersumber dari rechtsidee (cita hukum) bangsa Indonesia yaitu, Pancasila dan Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Djatmiko, 2022).

Berdasarkan kesesuaian konsep dari pengaturan keamanan siber dengan Pancasila sebagai dasar konstitusi Negara. Konsep pengaturan dari keamanan siber perlu juga sesuai dengan tujuan nasional Negara Indonesia yang ada dalam Pembukaan UUD 1945. Maka dalam pengaturan keamanan siber ini, kesesuaian UndangUndang Keamanan Siber dengan landasan filosofis cita hukum bangsa Indonesia adalah sebagai berikut:

1. Untuk mewujudkan tujuan nasional sebagaimana diamanatkan dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, aneka upaya multi sektoral untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia, perlu diberikan pengamanan dari berbagai bahaya akibat penyalahgunaan sarana dan prasarana atau sumber daya siber;
2. Segenap potensi sumber daya siber nasional untuk melakukan pengamanan terhadap kepentingan siber Indonesia, baik yang berada di sektor pemerintahan maupun yang berada di sektor swasta, perlu disinergikan dan diberikan peran yang
3. Penyeleggaraan pengamanan di bidang siber perlu disusun dalam suatu undang-undang agar pelaksanaan kekuasaan pemerintahan selaras dengan kepentingan perlindungan hak asasi manusia, kepentingan inovasi ilmu pengetahuan dan teknologi, serta kepentingan pemajuan perekonomian nasional;

Ancaman tambahan pada era yang ada sekarang ini mendorong potensi perang antar Negara tidak lagi menggunakan cara perang tradisional dan konvensional. Bentuk dari peperangan pun

berubah yang menimbulkan ancaman baru pada ruang siber yang dapat mengancam pertahanan, keamanan dan kedaualatan Negara (Rahmawati, 2017).

Pada suatu RUU juga akan dilihat pada Landasan yuridis, yang dimana peraturan perundang-undangan dapat dikatakan merupakan pertimbangan atau alasan yang menggambarkan bahwa peraturan yang dibentuk dapat mengatasi permasalahan hukum atau mengisi kekosongan hukum dengan mempertimbangkan peraturan-peraturan yang telah ada, yang akan diubah atau yang akan dicabut guna menjamin kepastian hukum dan rasa keadilan masyarakat (Laia & Daliwu, 2022). Terkait dengan landasan yuridis dalam undang-undangan keamanan siber, sesuai dengan ketentuan yang ada dalam Pasal 10 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan, materi muatan yang harus diatur dalam undang-undang berisi mengenai, pengaturan lebih lanjut mengenai ketentuan UUD 1945, perintah suatu undang-undang untuk diatur dengan undang-undang, pengesahan perjanjian internasional tertentu, tindak lanjut atas putusan Mahkamah Konstitusi, serta pemenuhan kebutuhan hukum dalam masyarakat. Peratuan perundang-undangan ini digunakan sebagai acuan dalam pembuatan suatu peraturan perundang-undangan lainnya.

Ketentuan yang ada tersebut menjadi suatu kesesuaian bahwa dalam undang-undang keamanan siber materi muatan yang terkandung berisi mengenai ketentuan lebih lanjut dari UUD 1945 yaitu dalam Pasal 30 UUD 1945 yang menyatakan bahwa segala hal yang terkait dengan pertahanan dan keamanan Negara diatur dengan undang-undang. Amanat lain mengenai materi muatan isi dari sebuah undang-undang adalah bahwa undang-undang keamanan siber dirasakan urgensinya dalam pemenuhan kebutuhan hukum untuk masyarakat. Atas segala pemanfaatan ruang siber atau internet yang telah menyetuh berbagai aspek kehidupan masyarakat termasuk pada infrastruktur kritis dan berbagai potensi ancaman kejahatan siber yang mampu memberikan dampak yang begitu luas pada masyarakat dan Negara Indonesia, maka kebutuhan dalam membuat undang-undang keamanan siber menjadi penting untuk dilaksanakan.

Saat ini pengaturan yang berkaitan dengan keamanan siber belum secara khusus diatur dan masih tersebar pada beberapa peraturan perundangan-undangan yang masih bersifat sektoral dan parsial. Hal ini seperti yang telah dijabarkan pada bab sebelumnya, materi muatan pengaturan keamanan siber tersebar dalam beberapa peraturan perundangan-undangan seperti: 1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi 2) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia 3) Undang-Undang Nomor 3 Tahun 2002 tentang Pertahan Negara 4) Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia 5) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara 6) Undang-Undang Nomor 3 Tahun 2014 tentang Perindustrian 7) Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Dapat dikatakan bahwa pengaturan yang ada tentang keamanan siber di Indonesia masih belum komprehensif atau bahkan undang-undang yang bersifat mengatur upaya keamanan siber yang mengaitkan antara pihak-pihak yang perlu memiliki tanggung jawab dalam berbagai upaya dari keamanan siber seperti pemerintah, masyarakat serta pihak swasta masih belum ada. Suatu peraturan yang berisi menyangkut hak dan kewajiban pemerintah, individu, pihak swasta, dan masyarakat dalam kaitannya dengan keamanan siber, aturan pencegahan dan penindakan terhadap penyalahgunaan pemanfaatan siber, serta tata hubungan dan koordinasi antara lembaga-lembaga pemerintah yang terkait, belum diatur secara jelas dan kuat secara hierarki.

Pada Prinsip Perlindungan Hukum dalam RUU KKS dilihat dari, Kepastian Hukum bahwa menuntut adanya aturan yang jelas, tidak multitafsir, serta dapat ditegakkan secara konsisten. berusaha menciptakan kepastian hukum dengan menegaskan definisi keamanan dan ketahanan siber, kewenangan Badan Siber dan Sandi Negara (BSSN), serta pengaturan standar keamanan siber bagi sektor publik maupun privat. Namun, potensi masalah muncul jika ketentuan dalam RUU terlalu umum, misalnya penggunaan istilah "ancaman terhadap keamanan nasional" yang tidak dirinci secara limitatif. Hal ini dapat menimbulkan multitafsir dan berpotensi disalahgunakan. Dengan demikian, meskipun RUU memberikan kerangka hukum, kepastian hukum baru dapat terwujud apabila norma-norma di dalamnya dijabarkan secara jelas dan teknis.

Pada Prinsip keadilan menghendaki agar perlindungan hukum diberikan secara seimbang, baik kepada negara maupun masyarakat. RUU KKS berupaya melindungi kepentingan nasional dari

ancaman siber, sekaligus melindungi hak-hak individu, seperti data pribadi dan kebebasan dari serangan siber. Namun, terdapat potensi ketidakseimbangan apabila kewenangan negara terlalu dominan, misalnya dalam pengawasan lalu lintas data tanpa mekanisme pengawasan independen. Agar prinsip keadilan terpenuhi, RUU perlu menjamin adanya mekanisme check and balance, misalnya melalui peran lembaga independen atau pengadilan dalam mengawasi tindakan negara.

RUU KKS Hukum harus membawa manfaat nyata bagi masyarakat luas, bukan hanya kepentingan negara. Manfaat positif dari RUU KKS adalah peningkatan kepercayaan masyarakat terhadap transaksi digital, perlindungan infrastruktur vital, serta kepastian hukum bagi pelaku usaha di bidang teknologi. Manfaat bagi negara adalah penguatan ketahanan nasional dan diplomasi siber internasional.

IV. KESIMPULAN

RUU Keamanan dan Ketahanan Siber memiliki urgensi strategis untuk menjawab meningkatnya ancaman kejahatan siber yang berpotensi mengganggu stabilitas politik, ekonomi, serta pertahanan dan keamanan negara. Pengaturan hukum yang ada saat ini, seperti UU ITE dan regulasi sektoral lainnya, masih bersifat parsial dan belum mampu memberikan perlindungan komprehensif terhadap infrastruktur kritis maupun data strategis nasional. RUU ini diharapkan dapat menjadi landasan hukum yang lebih tegas, jelas, dan konsisten dalam menjamin kepastian hukum, keadilan, serta kemanfaatan bagi masyarakat. Namun demikian, potensi permasalahan yuridis tetap ada, terutama terkait multitafsir norma, dominasi kewenangan negara, serta keterbatasan mekanisme pengawasan independen. Oleh karena itu, penyusunan RUU perlu memperhatikan asas keterpercayaan, kesiagaan, dan kolaboratif agar sejalan dengan Pancasila, UUD 1945, serta cita hukum bangsa. Dengan demikian, regulasi ini dapat benar-benar memperkuat kedaulatan digital Indonesia sekaligus melindungi hak-hak masyarakat di ruang siber.

REFERENSI

Amiruddin, Z. A. (2016). Pengantar metode penelitian hukum edisi revisi. Raja Grafindo Persada.

Arief, M. (2022). Urgensi regulasi ketahanan dan keamanan siber dalam Undang-Undang ITE. Jurnal Litigasi Amsir, 45-49. https://journalstih.amsir.ac.id/index.php/julia/article/view/127

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. Technology and Economics Law Journal, 2(2). https://scholarhub.ui.ac.id/telj/vol2/iss2/3

Buzan, B., & Hansen, L. (2009). The evolution of international security studies. Cambridge University Press.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rekonstruksi hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia. Dame Journal of Law, 1(1), 1-23.

Damayanti, D., & Ismowati, M. (2021). The implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta. ICSTIAMI. https://doi.org/10.4108/eai.17-7-2019.2302054

Djatmiko, W. P. (2022). Budaya hukum: Dalam masyarakat pluralistik. Dr. Wahyu Prijo Djatmiko.

Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society, 6(1). https://doi.org/10.1177/2053951719860542

Fitrah, E. (2015). Gagasan human security dan kebijakan keamanan nasional Indonesia. INSIGNIA: Journal of International Relations, 2(01), 27-41.

Halim, C., & Prasetyo, H. (2018). Penerapan artificial intelligence dalam Computer Aided Instructure (CAI). Jurnal Sistem Cerdas, 1(1). https://doi.org/10.37396/jsc.v1i1.6

Irwansyah, I., & Yunus, A. (2020). Penelitian hukum: Pilihan metode & praktik penulisan artikel. Mirra Buana Media.

Jamil, M. F. A., & Agussalim, A. (2025). Strategi siber Indonesia dalam kerja sama ASEAN untuk menjaga kedaulatan digital. Jurnal Ilmu Komunikasi, Administrasi Publik dan Kebijakan Negara, 2(3), 45–55. https://doi.org/10.62383/komunikasi.v2i3.421

Laia, S. W., & Daliwu, S. (2022). Urgensi landasan filosofis, sosiologis, dan yuridis dalam pembentukan undang-undang yang bersifat demokratis di Indonesia. Jurnal Education and Development, 10(1), 546-552.

Lasswell, H. D. (2017). Power and society: A framework for political inquiry. Routledge.

Maharani, M. A., & Atman, W. (2025). Evaluasi strategi nasional keamanan siber Indonesia dalam menanggapi ancaman digital Indonesia. Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik, 2(3), 344–354. https://doi.org/10.62383/sosial.v2i3.2291

Manurung, Y. S. (2024). Konsepsi kebijakan strategis pengelolaan nikel di era artificial intelligence dalam mendukung teknologi kedirgantaraan. Indonesian Journal of Innovation Multidisipliner Research, 2(2), 343-368.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense. Jurnal Pertahanan dan Bela Negara, 7(2), 35-50. https://doi.org/10.33172/jpbh.v7i2.179

Rongiyati, S. (2021). Urgensi sinergitas pengaturan perlindungan data pribadi dan keamanan siber nasional. Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis, 13(11), 1-6.

Sakban, A., Sahrul, A. K., & Tahir, H. (2020). The implementation repressive method to solving of cyber-bullying in the West Nusa Tenggara. International Journal of Advanced Science and Technology, 29(05), 13414-13421.

Santhi, N. N. P. P., & Nuarta, I. N. (2023). Penguatan penegakan hukum polri dalam rangka optimalisasi penanggulangan cybercrime di Indonesia. SCIENTIA: Journal of Multi Disciplinary Science, 2(1), 15-27. https://doi.org/10.62394/scientia.v2i1.40

Saputra, I. E., & Rahman, A. (2024). Reformasi sistem perundang-undangan Indonesia: Strategi pembentukan lembaga independen untuk menangani hiper-regulasi. JAPHTN-HAN, 3(1), 69–88. https://doi.org/10.55292/japhtnhan.v3i1.159

Saputri, D. P., Surryanto, D. W., & Risman, H. (2020). Indonesian cyber diplomacy: ASEAN-Japan online cyber exercise. Technium Social Sciences Journal, 9, 510-520.

Sihotang, H. T. M., Putri, M. A., Riwanda, N., & Nurbaity. (2025). Pentingnya keamanan data pada bisnis digital: Regulasi, tantangan, dan implementasi di Indonesia. Jebital: Jurnal Ekonomi dan Bisnis Digital, 2(2), 34-48.

Sugiartha, I. N. G., Dewi, A. A. S. L., & Widyantara, I. M. M. (2021). Law enforcement of fraud through electronic media. Sociological Jurisprudence Journal, 4(1), 61-67.

Unizar. (2025). Unizar soroti kebocoran pusat data nasional tantangan dan solusi bagi keamanan cyber di Indonesia. https://unizar.ac.id/unizar-soroti-kebocoran-pusat-data-nasional-tantangan-dan-solusi-bagikeamanan-cyber-di-indonesia/

Widjajanto, A., Perwita, A. A. B., Rezasyah, T., & Hersutanto, B. (2013). Penataan kebijakan keamanan nasional. Dian Cipta.