Bulletin of Community Engagement
Vol. 4, No. 3, December 2024
https://attractivejournal.com/index.php/bce/

Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang

H. Ajamalus[1], Agung Cucu Purnawirawan[1]
[1] *Sekolah Tinggi Ilmu Ekonomi Syariah Nahdlatul Ulama Bengkulu, Indonesia*

hajamalus@gmail.com

ARTICLE INFO
Article history:
Received
Revised
October 04, 2024
Accepted
October 27, 2024

Abstract

The development of digital technology has brought substantial transformation to various aspects of life, including in the legal realm. In Indonesia, cyber law has experienced significant developments to overcome challenges that arise along with changes in technology and people's behavior in the digital space. These challenges include issues of cyber security, personal data protection, as well as increasingly complex cyber crimes. To respond to these challenges, Indonesia has made adjustments to the legal framework, including a revision of the ITE Law, which aims to increase protection for internet users and strengthen law enforcement in the cyber context. Although there are a number of obstacles such as competency gaps and legal adaptation to rapidly developing technology, these developments also provide great opportunities for digital economic growth and national cyber security.

Keywords: Development of Cyber Law, Cyber Law, Cyber Law in Indonesia

Published by CV. Creative Tugu Pena
ISSN 2774-7077
Website https://attractivejournal.com/index.php/bce/

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan pada berbagai aspek kehidupan masyarakat. Salah satunya adalah munculnya ruang cyber atau dunia maya, yang menjadi tempat interaksi, bisnis, pendidikan, dan aktivitas lainnya. Meskipun membawa banyak manfaat, perkembangan teknologi ini juga menyimpan potensi risiko dan tantangan, termasuk kejahatan cyber yang semakin meningkat.

Hukum Cyber, atau yang juga dikenal sebagai Hukum Teknologi Informasi, adalah rangkaian peraturan, prinsip, dan standar hukum yang mengatur penggunaan internet dan teknologi terkait. Hukum ini dirancang untuk mengatasi masalah yang berhubungan dengan keamanan jaringan, akses data, privasi, perlindungan hak cipta, dan transaksi elektronik (Murray, 2023). Selain itu, hukum cyber juga bertujuan untuk melindungi penggunaan teknologi dari kejahatan seperti hacking, penipuan online, pencurian identitas, dan penyebaran virus. Dengan berkembang pesatnya teknologi digital, hukum cyber menjadi sangat penting untuk memastikan bahwa kegiatan di ruang digital aman dan teratur, serta hak dan privasi pengguna terlindungi (Holivia & Suratman, 2021).

Di era digital saat ini, keberadaan hukum cyber menjadi semakin penting karena hampir semua aspek kehidupan masyarakat berinteraksi dengan teknologi informasi dan komunikasi. Transaksi keuangan, komunikasi sosial, pendidikan, hiburan, dan bisnis secara luas telah beralih ke platform digital, menciptakan peluang besar untuk pertumbuhan ekonomi dan inovasi (Moulin, 2023). Namun, ini juga menimbulkan risiko dan tantangan baru, termasuk penyalahgunaan data pribadi, penipuan online, serangan cyber, dan pelanggaran hak cipta. Dalam konteks ini, hukum cyber berperan sebagai

kerangka kerja yang mengatur perilaku dalam ruang digital, menetapkan hak dan kewajiban bagi pengguna, serta menyediakan mekanisme perlindungan terhadap tindakan berbahaya atau ilegal. Kehadirannya penting untuk membangun kepercayaan pada sistem digital, yang menjadi kunci keberhasilan transformasi digital di berbagai sektor (Watt, 2021). Selain itu, hukum cyber juga penting untuk mendukung inovasi dan pertumbuhan ekonomi secara berkelanjutan. Dengan memastikan lingkungan digital yang aman dan terpercaya, hukum cyber memberikan dasar yang solid untuk perkembangan e-commerce, startup teknologi, serta investasi di bidang teknologi informasi. Ini membantu menciptakan ekosistem digital yang kondusif bagi inovasi, di mana hak kekayaan intelektual dilindungi, transaksi dibuat lebih transparan dan aman, serta dampak negatif dari teknologi dapat diminimalisir (Easttom, 2020). Melalui kerangka hukum yang jelas, pengusaha dan investor dapat lebih percaya diri dalam mengembangkan produk dan layanan baru, menyediakan landasan yang kuat bagi kemajuan ekonomi digital. Pada akhirnya, hukum cyber tidak hanya melindungi pengguna dan data mereka tetapi juga mendukung penciptaan nilai ekonomi dan sosial dalam ekosistem digital (Ganta, 2024).

Di Indonesia, kasus kejahatan cyber telah menunjukkan tren yang mengkhawatirkan. Dari penipuan online, pencurian identitas, hingga penyebaran konten ilegal dan berbahaya, kasus-kasus ini menimbulkan kerugian yang tidak hanya material tetapi juga psikologis bagi masyarakat. Keadaan ini mendesak perlunya regulasi yang memadai untuk mengatur ruang cyber, melindungi hak dan privasi warga negara, serta memastikan keamanan cyber nasional (Buchan & Navarrete, 2020). Akan tetapi, pengembangan hukum cyber di Indonesia menghadapi sejumlah tantangan. Antara lain adalah kecepatan perkembangan teknologi yang jauh melampaui proses pembuatan dan revisi regulasi, minimnya kesadaran dan pemahaman masyarakat tentang hukum dan keamanan cyber, serta keterbatasan sumber daya manusia yang kompeten di bidang penegakan hukum cyber (Watt, 2021).

Dalam konteks ini, mengevaluasi perkembangan hukum cyber di Indonesia menjadi sangat penting. Penelitian ini mengkaji tentang sejauh mana regulasi yang ada telah mengakomodasi kebutuhan perlindungan di ruang cyber, mengidentifikasi celah dan tantangan dalam implementasi hukum tersebut, serta menjajaki peluang untuk perbaikan dan pengembangan hukum cyber yang lebih efektif dan responsif terhadap perkembangan zaman.

METODE PENELITIAN

Kajian pada penelitian ini menggunakan metode penelitian literatur. Metode penelitian literatur merupakan salah satu pendekatan yang digunakan dalam penelitian akademik untuk mengumpulkan, menganalisis, dan menafsirkan data dari sumber-sumber tertulis, seperti buku, artikel jurnal, tesis, dan sumber online (Hidayat, 2009); (Afiyanti, 2008).

HASIL DAN PEMBAHASAN

Perkembangan Hukum Cyber di Indonesia

Hukum Cyber, atau yang sering juga disebut sebagai Hukum Teknologi Informasi, merujuk pada kumpulan prinsip hukum serta peraturan yang mengatur penggunaan dan akses terhadap teknologi informasi dan komunikasi. Dalam era digital yang terus berkembang ini, hukum cyber menjadi sangat penting untuk menangani isu-isu yang berkaitan dengan internet, teknologi digital, komputer, perangkat lunak, dan data (Abdukhalil & Dostonbek, 2024). Hal ini mencakup berbagai aspek seperti keamanan data, privasi online, hak cipta, transaksi elektronik, kejahatan cyber, dan tanggung jawab penyedia layanan internet. Tujuannya adalah untuk melindungi hak dan keamanan pengguna dalam ruang siber, seraya mempromosikan pertumbuhan dan inovasi dalam teknologi (Sunde, 2022).

Ruang lingkup Hukum Cyber sangat luas dan terus berkembang seiring dengan kemajuan teknologi. Isu-isu seperti fraud elektronik, pencurian identitas, penyebaran virus komputer, serangan ransomware, pelanggaran hak cipta melalui pembajakan digital, dan penyebaran konten ilegal adalah beberapa contoh masalah yang dibahas dalam hukum ini (Delerue, 2020). Selain itu, Hukum Cyber juga mencakup pembuatan regulasi untuk transaksi elektronik, tanda tangan digital, serta pengelolaan dan perlindungan data pribadi. Dengan meningkatnya ketergantungan masyarakat terhadap teknologi digital, pentingnya Hukum Cyber dalam menjaga keadilan, keamanan, dan penghormatan terhadap hak individu dan bisnis di dalam ekosistem digital menjadi semakin signifikan (Walters & Novak, 2021).

Perkembangan Hukum Cyber di Indonesia dapat ditandai dengan berbagai inisiatif legislatif dan kebijakan pemerintah yang bertujuan untuk menanggapi tantangan yang muncul dari evolusi teknologi informasi dan komunikasi. Salah satu tonggak penting dalam perkembangan hukum cyber di Indonesia adalah pengesahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016 (MANUILOV, 2023). UU ITE menyediakan kerangka hukum untuk transaksi elektronik, menyatakan hak dan kewajiban pengguna dan penyedia layanan internet, serta mengatur tentang tindak pidana di dunia maya, termasuk penyebaran konten ilegal dan pencemaran nama baik (Turns, 2021).

Selain UU ITE, Indonesia juga telah mengembangkan regulasi lainnya untuk mengatasi isu spesifik dalam dunia cyber, seperti pengaturan tentang keamanan data pribadi. Meski Indonesia belum memiliki undang-undang khusus mengenai perlindungan data pribadi, berbagai regulasi telah merintis jalan ke arah pengaturan yang lebih komprehensif, termasuk di dalamnya aturan-aturan yang disediakan oleh Kementerian Komunikasi dan Informatika serta kebijakan-kebijakan dari lembaga lainnya yang mengatasi aspek tertentu dari perlindungan data (Card, 2022).Penerapan hukum cyber di Indonesia juga melihat adanya peningkatan kerjasama antar lembaga pemerintah, baik di tingkat nasional maupun internasional, untuk mengatasi kejahatan cyber. Ini mencerminkan pemahaman bahwa kejahatan cyber seringkali bersifat transnasional, memerlukan respon yang terkoordinasi dan kolaboratif. Pemerintah Indonesia, melalui Kementerian Komunikasi dan Informatika, Polisi Republik Indonesia, dan lembaga terkait lainnya, telah berpartisipasi dalam berbagai inisiatif dan kerjasama internasional guna meningkatkan kapasitas dalam menangani masalah cybercrime (Moulin, 2023).

Namun, tantangan tetap ada. Perkembangan teknologi yang cepat memerlukan pemerintah untuk terus memperbarui dan menyempurnakan regulasi yang ada. Kritik dari masyarakat sipil seringkali berkisar pada isu hak asasi manusia, terutama terkait dengan kebebasan berekspresi online dan hak atas privasi. Di satu sisi, hukum harus cukup kuat untuk melindungi warga dari kejahatan dan penyalahgunaan di ruang siber. Di sisi lain, legislasi juga harus menghormati dan melindungi hak-hak fundamental warga negara. Keseimbangan ini menjadi tantangan yang berkelanjutan dalam evolusi hukum cyber di Indonesia (Tsagourias & Biggio, 2021).

Selanjutnya, dalam menghadapi perkembangan teknologi, khususnya di era digitalisasi yang semakin lanjut, Indonesia terus berupaya untuk memperkuat infrastruktur legal dan teknis dalam mencegah serta menanggulangi kejahatan cyber. Hal ini termasuk mempertimbangkan penciptaan undang-undang khusus yang menangani perlindungan data pribadi, yang telah lama menjadi topik diskusi di antara para pembuat kebijakan dan ahli teknologi (Grabowski & Robinson, 2021). Rencana untuk mengimplementasikan regulasi yang lebih ketat terkait penggunaan data pribadi menunjukkan komitmen Indonesia dalam menghadapi tantangan yang ditimbulkan oleh teknologi informasi dan komunikasi, serta internationalisasi kejahatan cyber (Wagner & Marusek, 2024).

Seiring dengan pengetatan regulasi, pemerintah juga meningkatkan upaya dalam peningkatan kesadaran dan pemahaman masyarakat tentang pentingnya keamanan data dan etika penggunaan internet. Pendidikan dan kampanye keamanan cyber menjadi bagian penting dalam strategi nasional untuk menciptakan ruang siber yang aman dan sehat bagi semua pengguna. Penguatan kerja sama antarlembaga dan dengan sektor privat juga dilakukan untuk mendukung sistem deteksi dan respon terhadap insiden cyber yang efisien, menunjukkan bahwa pendekatan komprehensif dan multi-stakeholder menjadi kunci dalam mengatasi tantangan cyber secara efektif (Bozgeyik, 2023).

Dengan demikian, perkembangan hukum cyber di Indonesia adalah bahwa perjuangan untuk menciptakan lingkungan siber yang aman dan sehat adalah proses yang berkelanjutan dan dinamis, menjawab tantangan yang timbul dari perkembangan teknologi informasi. Meskipun telah dilakukan banyak kemajuan, termasuk pengesahan UU ITE dan peningkatan kerja sama internasional dalam penanganan kejahatan cyber, masih ada ruang yang besar untuk peningkatan, khususnya dalam menyeimbangkan antara perlindungan terhadap hak individu dan kebutuhan untuk mengamankan ruang siber. Dengan demikian, pemerintah, industri, dan masyarakat harus terus bekerja sama dalam memperbarui dan meningkatkan hukum dan kebijakan, serta mempromosikan penggunaan teknologi yang bertanggung jawab dan etis demi kesejahteraan bersama.

Regulasi Hukum Cyber yang Berlaku di Indonesia

Di Indonesia, regulasi hukum yang mengatur tentang kejahatan di dunia maya dan penggunaan teknologi informasi secara umum adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE ini merupakan landasan hukum yang memberikan kerangka kerja bagi transaksi elektronik serta menetapkan berbagai jenis tindak pidana di dunia maya serta sanksinya, yang meliputi penyebaran konten ilegal, pelanggaran hak cipta, penipuan online, dan pencemaran nama baik melalui media elektronik (KAZMIRUK & LEONOV, 2023).

Selain UU ITE, terdapat pula beberapa regulasi pendukung lainnya yang berkaitan dengan aspek khusus penggunaan internet dan teknologi informasi, seperti UU Nomor 36 Tahun 1999 tentang Telekomunikasi, UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan UU Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Regulasi-regulasi ini berfungsi untuk melindungi pengguna dan penyedia layanan internet, serta memastikan bahwa pertukaran informasi dan transaksi elektronik berjalan dengan aman dan bertanggung jawab (Strupczewski, 2024).

Pada tahun 2020, pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika juga mulai membahas Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) sebagai jawaban atas semakin meningkatnya kebutuhan untuk melindungi data pribadi pengguna internet di Indonesia. RUU PDP diharapkan dapat mengisi kekosongan hukum terkait pengelolaan dan perlindungan data pribadi, yang selama ini bergantung pada peraturan-peraturan sektoral dan belum memiliki undang-undang khusus yang mengaturnya secara komprehensif (Utkirovich, 2023). Keberadaan dan pengembangan regulasi hukum cyber di Indonesia menunjukkan komitmen pemerintah dalam menghadapi tantangan dan peluang yang ditimbulkan oleh digitalisasi. Dalam praktiknya, penerapan hukum ini terus menerus diuji dan diperbarui untuk menyesuaikan dengan perkembangan teknologi yang sangat cepat (Leone, 2024). Oleh karena itu, kolaborasi antara pemerintah, industri, dan masyarakat sipil menjadi sangat penting untuk memastikan bahwa regulasi hukum cyber di Indonesia dapat efektif melindungi hak-hak pengguna sekaligus mendukung pertumbuhan ekonomi digital yang inklusif dan berkelanjutan.

Tantangan dalam penerapan dan penegakan hukum cyber

Penerapan dan penegakan hukum cyber di Indonesia menghadapi sejumlah tantangan signifikan yang disebabkan oleh berbagai faktor. Salah satu tantangan utama adalah sifat kejahatan siber itu sendiri, yang sering kali bersifat transnasional. Pelaku kejahatan dapat beroperasi dari negara mana pun, menargetkan korban di negara lain, termasuk Indonesia, yang membuat penegakan hukum menjadi sangat kompleks. Hal ini memerlukan kerja sama internasional yang erat antara penegak hukum di berbagai negara, namun koordinasi semacam itu sering kali dihambat oleh perbedaan kerangka hukum dan keterbatasan sumber daya (Nakane, 2024).

Selain itu, perkembangan teknologi informasi yang begitu cepat juga menjadi tantangan tersendiri. Regulasi yang ada mungkin segera menjadi usang dan tidak lagi relevan dengan praktik terkini di dunia maya. Misalnya, munculnya teknologi baru seperti artificial intelligence, blockchain, dan Internet of Things (IoT) membuka peluang baru bagi kejahatan siber yang mungkin belum sepenuhnya diantisipasi oleh hukum yang berlaku saat ini. Dengan demikian, diperlukan upaya untuk terus memperbarui dan menyesuaikan regulasi agar tetap relevan dengan perkembangan teknologi (Łągiewska, 2024). Lanjut lagi, tantangan berikutnya adalah keterbatasan kapasitas dan keahlian para penegak hukum dalam menghadapi kejahatan siber. Penyelidikan kejahatan siber menuntut pemahaman teknis yang tinggi serta akses ke peralatan dan teknologi yang canggih. Banyak kasus kejahatan siber yang tidak bisa diselesaikan karena penegak hukum kekurangan alat bukti digital yang memadai atau keahlian untuk menganalisisnya (Dubovyk, 2020). Hal ini menunjukkan pentingnya investasi dalam pembangunan kapasitas lembaga penegakan hukum, termasuk pelatihan personel dalam teknologi informasi dan forensik digital. Selain itu, kesadaran masyarakat Indonesia terkait keamanan siber juga masih rendah. Banyak pengguna internet yang tidak menyadari pentingnya menjaga keamanan data pribadi mereka atau ternyata mudah terperdaya oleh penipuan online. Pendidikan dan kampanye kesadaran tentang keamanan siber sangat diperlukan untuk meningkatkan kewaspadaan Masyarakat (Hayashi & Letrône, 2021). Tanpa partisipasi aktif dari masyarakat, upaya penegakan hukum saja tidak akan cukup untuk mengatasi kejahatan siber. Oleh karena itu, perlu ada sinergi antara pemerintah, industri, dan masyarakat untuk bersama-sama mengatasi tantangan keamanan siber.

Kesemuanya, tantangan dalam penerapan dan penegakan hukum cyber di Indonesia memerlukan pendekatan yang komprehensif dan kolaboratif. Hal ini mencakup perbaikan regulasi agar tetap relevan, peningkatan kapasitas lembaga penegak hukum, serta peningkatan kesadaran masyarakat tentang keamanan siber. Dengan menghadapi tantangan-tantangan ini secara bersama, Indonesia dapat mengembangkan lingkungan siber yang aman dan kondusif untuk semua pengguna.

Pemanfaatan teknologi untuk penegakan hukum cyber

Teknologi memainkan peran penting dalam penegakan hukum di ranah cyber, terutama karena aktivitas kejahatan siber sering kali dapat berlangsung secara anonim dan menyeberangi batas geografis. Salah satu pemanfaatan teknologi adalah melalui penggunaan perangkat lunak forensik digital yang canggih. Aplikasi semacam ini memungkinkan penegak hukum untuk mengumpulkan dan menganalisis bukti digital dari berbagai sumber, mencakup komputer, ponsel pintar, server, dan jaringan. Teknologi ini bertujuan untuk mengidentifikasi, mengumpulkan, dan memelihara informasi de manière yang sesuai dengan prinsip hukum untuk memastikan bahwa informasi tersebut dapat digunakan di pengadilan (Kilovaty, 2021).

Selain itu, teknologi kecerdasan buatan (artificial intelligence, AI) dan pembelajaran mesin (machine learning) juga mulai dimanfaatkan untuk mendeteksi pola-pola kejahatan siber yang lebih cepat dan akurat (Das, 2021). AI dapat menganalisis sejumlah besar data untuk mengidentifikasi aktivitas mencurigakan secara real-time dan membantu penegak hukum dalam mengambil tindakan pencegahan atau penindakan lebih

cepat dari sebelumnya. Pemanfaatan AI dalam sistem keamanan siber memungkinkan analisis yang lebih dalam atas perilaku jaringan dan mencari deviasi yang mungkin menunjukkan adanya serangan (Mukati & Prakash, 2022).

Adapun, teknologi blockchain menawarkan kemungkinan untuk mengamankan rantai bukti digital dan meningkatkan integritas data yang digunakan dalam penyelidikan. Dengan menggunakan teknologi desentralisasi yang diberikan oleh blockchain, bukti digital dapat dicatat dalam bentuk yang tidak dapat diubah tanpa konsensus, sehingga mengurangi risiko penghapusan atau manipulasi bukti yang mungkin dilakukan oleh pelaku kejahatan. Hal ini sangat bermanfaat dalam memastikan keaslian bukti yang diperoleh dari ruang siber dan memperkuat kasus di pengadilan (Mačák, 2021). Terakhir, penggunaan jaringan komunikasi terenkripsi bagi penegak hukum dan pihak kehakiman memastikan bahwa informasi sensitif yang berkaitan dengan penyelidikan dapat dijaga kerahasiannya. Teknologi enkripsi berperan dalam melindungi pertukaran informasi antara lembaga penegak hukum, sehingga strategi dan operasi keamanan cyber tidak terkomprimitasi oleh pihak yang tidak diinginkan. Teknologi ini juga penting untuk menjaga privasi dan hak asasi masyarakat dalam konteks penegakan hukum sehingga tidak terjadi penyalahgunaan data.

Dengan demikian, teknologi memiliki dampak yang signifikan dalam membantu penegak hukum cyber dalam melaksanakan tugasnya. Penerapan teknologi forensik digital, AI, blockchain, dan enkripsi, ketika diintegrasikan dengan baik, dapat memberikan keunggulan yang signifikan dalam memerangi kejahatan siber, memperkuat riwayat bukti, dan melindungi informasi yang sensitif serta infrastruktur dari potensi kompromi atau serangan.

KESIMPULAN

Perkembangan hukum cyber di Indonesia menandai periode penting dalam upaya menghadapi tantangan yang ditimbulkan oleh kemajuan teknologi serta ekspansi ruang digital. Implementasi hukum di bidang cyber tidak hanya terfokus pada penegakan, tetapi juga mencakup perlindungan data pribadi, transaksi online, dan keamanan siber untuk individu serta entitas bisnis. Hal ini mencerminkan respons proaktif pemerintah dalam menciptakan lingkungan digital yang aman dan terpercaya. Meski demikian, berbagai tantangan seperti perubahan cepat dalam teknologi, kejahatan siber yang semakin kompleks, serta kesenjangan pengetahuan hukum dan teknologi di kalangan penegak hukum menjadi hambatan yang mesti diatasi. Untuk merespons tantangan tersebut, Indonesia telah melakukan sejumlah penyesuaian dan pembaruan pada kerangka hukumnya. Pembaruan hukum tersebut mencakup penyesuaian terhadap UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) yang menjadi pondasi hukum cyber di Indonesia. Penyesuaian ini bertujuan untuk mengakomodasi dinamika baru dalam transaksi digital dan kejahatan siber, sekaligus memperkuat perlindungan bagi pengguna internet di Indonesia. Namun, keberhasilan implementasi hukum tersebut sangat tergantung pada pemahaman dan adaptasi dari semua pihak terkait, termasuk masyarakat umum. Dari sisi peluang, perkembangan hukum cyber di Indonesia membuka jalan bagi peningkatan keamanan siber nasional dan mendorong pertumbuhan ekonomi digital. Aspek legal yang kuat dan jelas menjadi fondasi yang penting bagi investor dan pelaku bisnis untuk memasuki dan berkembang di pasar Indonesia. Selain itu, peningkatan kapasitas penegak hukum dalam menangani kejahatan siber dapat menambah kepercayaan publik terhadap penggunaan layanan digital, yang pada gilirannya, dapat memacu inovasi dan inklusi digital lebih lanjut. Sebagai kesimpulan, perkembangan hukum cyber di Indonesia menunjukkan komitmen yang kuat dari pemerintah dalam menanggapi dinamika global yang ditimbulkan oleh teknologi digital. Meski dihadapkan pada berbagai tantangan, adaptasi hukum dan peningkatan kapasitas penegak hukum menunjukkan progress positif menuju ekosistem digital yang aman dan inklusif. Dengan

melihat ke depan, sinergi antara pembaruan hukum, pengembangan teknologi, dan edukasi masyarakat menjadi kunci dalam mengoptimalkan peluang yang ditawarkan oleh era digital, sekaligus meminimalisir risikonya bagi Indonesia.

REFERENSI

Abdukhalil, G., & Dostonbek, T. (2024). CYBER INTELLIGENCE PRACTICE IN PREVENTING CYBER THREATS AND ITS PRIORITIES. *Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations*, *1*(6), 31–36. https://doi.org/10.61796/ejcblt.v1i6.653

Afiyanti, Y. (2008). Focus Group Discussion (Diskusi Kelompok Terfokus) sebagai Metode Pengumpulan Data Penelitian Kualitatif. *Jurnal Keperawatan Indonesia*, *12*(1), 58–62. https://doi.org/10.7454/jki.v12i1.201

Bozgeyik, H. (2023). Importance of Cyber Law. *Uzbek Journal of Law and Digital Policy*, *2*(2). https://doi.org/10.59022/ujldp.104

Buchan, R., & Navarrete, I. (2020). Cyber Espionage. *International Law*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.1093/obo/9780199796953-0212

Card, R. (2022). Cyber-Crime and Computer Misuse. *Card and English on Police Law*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.1093/law/9780192866165.003.0015

Das, I. (2021). The Outer Space and Cyber-Attacks: How India's Proposed National Space Law Deals with Cyber-Security. *International Institute of Space Law*, *64*(5), 303–314. https://doi.org/10.5553/iisl/2021064005002

Delerue, F. (2020). *Cyber Operations and International Law*. *Query date: 2024-10-05 21:13:28*. https://doi.org/10.1017/9781108780605

Dubovyk, V. B. (2020). ROLE OF OSCE IN ENSURING CYBER SECURITY. *Law Bulletin*, *12*, 87–91. https://doi.org/10.32850/lb2414-4207.2020.12.12

Easttom, C. (2020). Criminal Law. *The NICE Cyber Security Framework*, *Query date: 2024-10-05 21:13:28*, 79–97. https://doi.org/10.1007/978-3-030-41987-5_4

Ganta, S. K. (2024). *Cyber crime and cyber law in india—A strategic perspective*. *Query date: 2024-10-05 21:13:28*. https://doi.org/10.58673/sp.2024.06.13.01

Grabowski, M., & Robinson, E. P. (2021). Emerging Issues in Cyber Law. *Cyber Law and Ethics*, *Query date: 2024-10-05 21:13:28*, 208–222. https://doi.org/10.4324/9781003027782-12

Hayashi, M., & Letrône, W. (2021). State-sponsored cyber operations and international law: Book review of Henning Lahmann, Unilateral Remedies to Cyber Operations (Cambridge University Press, 2020) and François Delerue, Cyber Operations and International Law (Cambridge University Press, 2020). *International Cybersecurity Law Review*, *2*(1), 195–200. https://doi.org/10.1365/s43439-021-00031-w

Hidayat, D. N. (2009). DIKOTOMI KUALITATIF – KUANTITATIF DAN VARIAN PARADIGMATIK DALAM PENELITIAN KUALITATIF. *Scriptura*, *2*(2). https://doi.org/10.9744/scriptura.2.2.81-94

Holivia, A., & Suratman, T. (2021). Child Cyber Grooming Sebagai Bentuk Modus Baru Cyber Space Crimes. *Bhirawa Law Journal*, *2*(1), 1–13. https://doi.org/10.26905/blj.v2i1.5847

KAZMIRUK, S., & LEONOV, B. (2023). Legal and organizational provision of cyber protection of lie detection systems against cyber attacks under the conditions of the martial law. *INFORMATION AND LAW*, *3*, 135–141. https://doi.org/10.37750/2616-6798.2023.3(46).287217

Kilovaty, I. (2021). The international law of cyber intervention. *Research Handbook on International Law and Cyberspace*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.4337/9781789904253.00014

Łągiewska, M. (2024). Online Hate Speech Under International Law. *Law and Visual Jurisprudence*, *Query date: 2024-10-05 21:13:28*, 301–312. https://doi.org/10.1007/978-3-031-51248-3_15
Leone, M. (2024). On Cyber-Envy. *Law and Visual Jurisprudence*, *Query date: 2024-10-05 21:13:28*, 15–34. https://doi.org/10.1007/978-3-031-51248-3_2
Mačák, K. (2021). Unblurring the lines: Military cyber operations and international law. *Journal of Cyber Policy*, *6*(3), 411–428. https://doi.org/10.1080/23738871.2021.2014919
MANUILOV, Y. (2023). Cyber security of critical infrastructure during cyber warfare. *INFORMATION AND LAW*, *1*, 154–167. https://doi.org/10.37750/2616-6798.2023.1(44).287780
Moulin, T. (2023). Collective security law. *Cyber-Espionage in International Law*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.7765/9781526168047.00013
Mukati, A., & Prakash, Dr. S. (2022). The Role of Data Leakage Prevention System in CBDC. *Indian Journal of Cryptography and Network Security*, *2*(2), 5–11. https://doi.org/10.54105/ijcns.b3604.112222
Murray, A. (2023). 5. Cyber-speech. *Information Technology Law*, *Query date: 2024-10-05 21:13:28*, 95–132. https://doi.org/10.1093/he/9780192893529.003.0005
Nakane, I. (2024). Online Discrimination Based on COVID-19: A Language and Law Perspective. *Law and Visual Jurisprudence*, *Query date: 2024-10-05 21:13:28*, 357–384. https://doi.org/10.1007/978-3-031-51248-3_18
Strupczewski, G. (2024). Mitigating Cyber Risk in Personal Finance of the Elderly. Insights into Vulnerabilities, Cyber Hygiene and the Role of Personal Cyber Insurance. *Cybersecurity and Law*, *11*(1), 281–298. https://doi.org/10.35467/cal/188460
Sunde, I. M. (2022). Cyber Investigation Law. *Cyber Investigations*, *Query date: 2024-10-05 21:13:28*, 51–73. https://doi.org/10.1002/9781119582021.ch3
Tsagourias, N., & Biggio, G. (2021). Cyber-peacekeeping and international law. *Research Handbook on International Law and Cyberspace*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.4337/9781789904253.00027
Turns, D. (2021). Cyber war and the law of neutrality. *Research Handbook on International Law and Cyberspace*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.4337/9781789904253.00034
Utkirovich, R. U. (2023). Navigating the Cyber Legal Landscape: Protecting Legal Entities through Comprehensive Cyber-security Strategies. *Uzbek Journal of Law and Digital Policy*, *1*(1). https://doi.org/10.59022/ujldp.56
Wagner, A., & Marusek, S. (2024). Handbook on Cyber Hate. In *Law and Visual Jurisprudence*. Springer International Publishing. https://doi.org/10.1007/978-3-031-51248-3
Walters, R., & Novak, M. (2021). Cyber Security. *Cyber Security, Artificial Intelligence, Data Protection & the Law*, *Query date: 2024-10-05 21:13:28*, 21–37. https://doi.org/10.1007/978-981-16-1665-5_2
Watt, E. (2021). Cyber espionage, cyber surveillance, foreign electoral interference and international law. *State Sponsored Cyber Surveillance*, *Query date: 2024-10-05 21:13:28*. https://doi.org/10.4337/9781789900101.00007