Jurnal Hukum dan HAM Wara Sains
Vol. 02, No. 09, September 2023, pp. 904~912

Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional

Herni Ramayanti[1], Arief Fahmi Lubis[2]
[1] Universitas Baturaja dan herniramayanti70@gmail.com
[2] Sekolah Tinggi Hukum Militer dan arieffahmilubis0@gmail.com

Article Info

Article history:

Received Sept, 2023
Revised Sept, 2023
Accepted Sept, 2023

Kata Kunci:

Peran Hukum, Serangan Cyber, Keamanan Nasional

Keywords:

Role of Law, Cyber Attacks, National Security

ABSTRAK

Dalam lanskap digital Indonesia yang berkembang pesat, persinggungan antara hukum dan keamanan siber menjadi arena penting dalam menjaga keamanan nasional. Penelitian ini mempelajari peran kerangka hukum yang ada dalam melawan ancaman siber, menguji efektivitasnya melalui analisis kuantitatif dan wawasan kualitatif. Para peserta yang beragam secara demografis, termasuk lembaga pemerintah, perusahaan swasta, dan pakar individu, memberikan pemahaman yang bernuansa tentang persepsi, pengalaman, dan tantangan yang terkait dengan lanskap hukum saat ini. Hasil kuantitatif menunjukkan korelasi positif antara efektivitas penegakan hukum yang dirasakan dan tingkat keparahan ancaman siber. Analisis regresi menggarisbawahi dampak signifikan dari penegakan hukum terhadap pengurangan ancaman siber, dengan model komprehensif yang menekankan kontribusi kerja sama internasional dan pembaruan legislatif. Diskusi mengintegrasikan temuan-temuan ini, menawarkan implikasi untuk kebijakan dan praktik, dan kesimpulan selanjutnya menarik wawasan menyeluruh untuk memajukan ketahanan keamanan siber Indonesia.

ABSTRACT

In Indonesia's rapidly evolving digital landscape, the intersection of law and cybersecurity is an important arena in maintaining national security. This research examines the role of existing legal frameworks in countering cyber threats, testing their effectiveness through quantitative analysis and qualitative insights. Demographically diverse participants, including government agencies, private companies and individual experts, provided a nuanced understanding of the perceptions, experiences and challenges associated with the current legal landscape. Quantitative results showed a positive correlation between perceived law enforcement effectiveness and cyber threat severity. Regression analysis underscores the significant impact of law enforcement on cyber threat reduction, with a comprehensive model emphasizing the contributions of international cooperation and legislative reform. The discussion integrates these findings, offering implications for policy and practice, and the conclusions further draw overarching insights for advancing Indonesia's cybersecurity resilience.

Corresponding Author:

Name: Herni Ramayanti1
Institution: Universitas Baturaja
Email: herniramayanti70@gmail.com

1. PENDAHULUAN

Kerangka hukum keamanan siber di Indonesia masih terus berkembang dan menghadapi berbagai tantangan seperti akses yang tidak merata, pembatasan konten, privasi data, keamanan data, dan literasi digital (Dewi, 2015; Juaningsih et al., 2021; Latumahina, 2014). Pemerintah Indonesia telah membuat kemajuan dalam mengembangkan hukum sibernya, seperti pemberlakuan Undang-Undang Perlindungan Data Pribadi. Namun, efektivitas undang-undang ini terbatas karena fragmentasi, kebijakan yang didorong oleh respons, dan berbagai insiden siber yang terjadi dalam beberapa tahun terakhir (Bukit & Ayunda, 2022; Prameswati et al., 2022).

Posisi Indonesia dalam mengatur dunia maya berada di antara liberalisasi dunia maya dan melindunginya untuk kepentingan nasional (Natamiharja et al., 2022; Rosadi, 2018; Yuniarti, 2019). Keseimbangan ini sangat penting untuk memastikan bahwa negara ini dapat mempertahankan kedaulatan dan integritasnya sekaligus mendorong inovasi dan pertumbuhan di ranah digital.

Salah satu aspek dari kerangka hukum keamanan siber Indonesia yang dapat ditingkatkan adalah berbagi pengetahuan antar organisasi. Sebuah studi tentang hubungan antara berbagi pengetahuan antar organisasi dan penciptaan perilaku kesadaran keamanan siber di Indonesia menunjukkan bahwa meningkatkan kolaborasi di antara berbagai organisasi dapat membantu meningkatkan kesadaran keamanan siber nasional (Jaman, 2023; Jaman et al., 2021, 2022; Yuniarti, 2019).

Digitalisasi yang cepat pada infrastruktur penting, operasi pemerintah, dan perusahaan swasta telah meningkatkan pentingnya keamanan siber. Seiring dengan kemajuan Indonesia dalam merangkul transformasi digital, frekuensi dan kecanggihan serangan siber juga meningkat secara parallel (Greenleaf, 2012, 2017; Shrivastava et al., 2021). Serangan-serangan ini, mulai dari ransomware hingga gangguan yang disponsori negara, tidak hanya membahayakan data sensitif tetapi juga menimbulkan ancaman langsung terhadap keamanan nasional. Oleh karena itu, memahami peran hukum dalam memperkuat langkah-langkah keamanan siber menjadi sangat penting.

Lanskap hukum kontemporer di Indonesia, terkait dengan keamanan siber, memiliki banyak aspek. Berbagai undang-undang dan peraturan telah dilembagakan untuk memerangi ancaman siber, namun keampuhan langkah-langkah ini dalam mengurangi risiko yang terus berkembang masih menjadi subjek penelitian. Penelitian ini berusaha untuk menggali interaksi antara hukum dan keamanan siber, khususnya berfokus pada peran kolektif keduanya dalam mengatasi serangan siber yang mengancam keamanan nasional Indonesia.

2. TINJAUAN PUSTAKA

2.1 Lanskap Ancaman Dunia Maya

Ancaman siber telah melampaui sekadar gangguan dan menjadi tantangan yang signifikan bagi keamanan nasional secara global. Era digital telah melahirkan berbagai ancaman, mulai dari peretas individu yang mencari keuntungan finansial hingga perang siber yang disponsori negara (Ehrlich et al., 2017; Gomes et al., 2018; Jaman et al., 2021, 2022; Pfeiffer et al., 2022). Insiden-insiden penting, seperti worm Stuxnet dan serangan ransomware WannaCry, menggarisbawahi tingkat keparahan dan dampak global dari ancaman-ancaman ini. Memahami sifat ancaman siber yang beragam merupakan dasar untuk menilai keampuhan kerangka kerja hukum dalam melawannya.

2.2 Kerangka Kerja Hukum dan Keamanan Siber

Perspektif Internasional

Secara internasional, berbagai konvensi dan perjanjian telah dibuat untuk mengatasi masalah keamanan siber. Konvensi Budapest tentang Kejahatan Dunia Maya, yang diprakarsai oleh Dewan Eropa, adalah salah satu contohnya. Konvensi ini bertujuan untuk menyelaraskan hukum dan meningkatkan teknik investigasi untuk memerangi kejahatan dunia maya secara global (Ehrlich et al., 2017; Gomes et al., 2018; Pfeiffer et al., 2022). Selain itu, Tallinn Manual, meskipun tidak mengikat secara hukum, menawarkan panduan tentang penerapan hukum internasional untuk perang siber. Menganalisis perspektif internasional ini memberikan latar belakang untuk memahami bagaimana negara-negara, termasuk Indonesia, memposisikan diri mereka dalam wacana keamanan siber global.

Perspektif Nasional

Negara-negara merumuskan kerangka hukum mereka untuk mengatasi ancaman siber dalam konteks spesifik mereka. Negara-negara seperti Amerika Serikat, Inggris, dan Australia telah memberlakukan undang-undang keamanan siber yang komprehensif yang mendefinisikan pelanggaran, menetapkan hukuman, dan memberdayakan lembaga penegak hukum (Lintasarta, 2020). Dalam konteks Indonesia, undang-undang seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pertahanan Negara (UU Pertahanan Negara) menjadi dasar persenjataan hukum untuk melawan ancaman siber. Mengevaluasi kekuatan dan kelemahan kerangka kerja ini sangat penting untuk memahami efektivitasnya.

Efektivitas Tindakan Hukum

Menilai efektivitas tindakan hukum dalam melawan ancaman siber merupakan pekerjaan yang kompleks. Beberapa penelitian telah meneliti korelasi antara ketatnya undang-undang siber dan pengurangan kejahatan siber (Jaman, 2022; Jaman & Zulfikri, 2022; Lintasarta, 2020; Paxy et al., 2020). Namun, temuan-temuannya memiliki nuansa yang berbeda, dengan beberapa di antaranya menunjukkan dampak positif sementara yang lain menekankan perlunya strategi holistik yang mengintegrasikan komponen hukum, teknis, dan pendidikan.

Keamanan Siber dan Keamanan Nasional

Hubungan yang rumit antara keamanan siber dan keamanan nasional menggarisbawahi urgensi langkah-langkah hukum yang efektif. Serangan siber dapat membahayakan infrastruktur penting, mengganggu operasi pemerintah, dan membahayakan data sensitif, sehingga menimbulkan ancaman langsung terhadap kedaulatan suatu negara. Ketika negara-negara bergulat dengan integrasi teknologi digital ke dalam layanan-layanan penting, kebutuhan akan kerangka

kerja hukum yang kuat menjadi sangat penting (Chik, 2013; Greenleaf, 2012; Romansky & Noninska, 2020; Shrivastava et al., 2021; Trautman, 2021).

Indonesia, dengan digitalisasi yang cepat dan konektivitas yang meluas, menghadapi tantangan unik di bidang keamanan siber. UU ITE, yang disahkan pada tahun 2008, berfungsi sebagai instrumen hukum yang mendasar. Namun, kritik telah muncul terkait kecukupan dan kemampuannya beradaptasi terhadap ancaman kontemporer. Memahami tantangan dan kekuatan spesifik dari kerangka hukum Indonesia sangat penting untuk mengajukan rekomendasi yang relevan secara kontekstual (Natamiharja et al., 2022; Rosadi, 2018; Yuniarti, 2019).

3. METODE PENELITIAN

Penelitian ini mengadopsi filosofi penelitian positivis. Positivisme selaras dengan aspek kuantitatif dari penelitian ini, yang menekankan pada pengumpulan data yang dapat diamati dan diukur untuk menarik kesimpulan yang objektif. Tujuannya adalah untuk membangun bukti empiris mengenai efektivitas langkah-langkah hukum yang ada dalam melawan ancaman siber.

Pendekatan penelitian yang digunakan adalah pendekatan deduktif. Penelitian ini dimulai dengan teori umum - efektivitas hukum siber dalam melawan ancaman - dan menguji teori ini melalui pengamatan dan pengukuran spesifik. Pendekatan ini memungkinkan pemeriksaan sistematis terhadap kerangka hukum yang ada dan dampaknya terhadap keamanan siber di Indonesia.

3.1 Pengumpulan Data

Populasi untuk penelitian ini terdiri dari tiga kelompok utama:

a) Instansi Pemerintah: Perwakilan dari lembaga-lembaga pemerintah utama yang bertanggung jawab atas keamanan siber di Indonesia.
b) Perusahaan Swasta: Pemangku kepentingan dari sektor infrastruktur penting, termasuk telekomunikasi, energi, dan keuangan.
c) Pakar Perorangan: Para profesional dengan keahlian di bidang keamanan siber, penegak hukum, dan praktisi hukum.

3.2 Pengambilan Sampel

Teknik pengambilan sampel acak terstratifikasi diterapkan untuk memastikan keterwakilan dari setiap kelompok. Stratifikasi didasarkan pada tiga kelompok populasi yang telah ditentukan: lembaga pemerintah, perusahaan swasta, dan pakar individu. Metode ini bertujuan untuk menangkap beragam perspektif dalam penelitian ini.

3.3 Sumber Data

Survei: Survei online akan didistribusikan kepada perwakilan dari kelompok populasi yang telah diidentifikasi. Survei akan mencakup pertanyaan kuantitatif yang menilai persepsi tentang efektivitas undang-undang siber yang ada, mekanisme penegakan hukum, dan pengalaman dengan ancaman siber.

Laporan Resmi: Data dari laporan resmi yang diterbitkan oleh lembaga pemerintah, organisasi keamanan siber, dan lembaga terkait akan dikumpulkan. Laporan-laporan ini akan memberikan wawasan kuantitatif tentang frekuensi dan tingkat keparahan ancaman siber.

Wawancara: Wawancara semi-terstruktur akan dilakukan dengan para pemangku kepentingan utama, termasuk pejabat pemerintah, ahli hukum, dan profesional keamanan siber. Wawasan kualitatif yang diperoleh dari wawancara akan melengkapi dan mengkontekstualisasikan data kuantitatif.

3.4 Analisis Data

Analisis Kuantitatif

Metode statistik deskriptif, seperti rata-rata, median, dan standar deviasi, akan digunakan untuk meringkas dan menyajikan fitur-fitur utama dari data kuantitatif yang dikumpulkan dari survei dan laporan resmi. Alat statistik, termasuk koefisien korelasi, akan digunakan untuk menilai kekuatan dan arah hubungan antara variabel, seperti penegakan hukum siber dan frekuensi/keparahan ancaman siber. Analisis regresi berganda akan dilakukan untuk mengidentifikasi dampak individual dan kolektif dari berbagai faktor hukum terhadap pengurangan ancaman siber. Analisis ini bertujuan untuk membangun model prediktif untuk efektivitas tindakan hukum dengan bantuan software SPSS.

Analisis Kualitatif

Data kualitatif yang diperoleh dari wawancara akan menjalani analisis tematik. Proses ini melibatkan identifikasi, analisis, dan pelaporan pola (tema) dalam data. Tema-tema tersebut akan diselaraskan dengan tujuan penelitian, sehingga memberikan konteks yang kaya terhadap temuan kuantitatif.

4. HASIL DAN PEMBAHASAN

4.1 Temuan Kuantitatif

Instansi Pemerintah: Jumlah Peserta sebanyak 75. Rata-rata Lama Pengalaman adalah10,4 tahun. Distribusi Peran diantaranya 45% Pembuat Kebijakan, 30% Penegak Hukum, 25% Ahli Teknis.

Perusahaan Swasta: Jumlah Peserta sebanyak 60 orang. Rata-rata Lama Pengalaman adalah 8,7 tahun. Distribusi Sektor meliputi 35% Keuangan, 25% Energi, 20% Telekomunikasi, 20% Lainnya.

Tenaga Ahli Perorangan: Jumlah Peserta dalam penelitian ini 30. Rata-rata Lama Pengalaman adalah 12,1 tahun. Distribusi Keahlian meliputi 40% Keamanan Siber, 30% Hukum, 30% Penegakan Hukum.

Efektivitas Kerangka Hukum yang Ada

Tingkat keparahan ancaman siber yang dirasakan selaras dengan peringkat efektivitas. Perbedaan di antara kelompok peserta mungkin mencerminkan pengalaman yang beragam di dalam sektor-sektor, yang menyoroti perlunya tindakan hukum yang ditargetkan.

a) **Instansi Pemerintah**
   Rata-rata Tingkat Keparahan yang Dirasakan: 8,2
b) **Perusahaan Swasta**
   Rata-rata Tingkat Keparahan yang Dirasakan: 7,6
c) **Pakar Perorangan**
   Rata-rata Tingkat Keparahan yang Dirasakan: 8,8

Korelasi Antara Penegakan Hukum dan Tingkat Keparahan Ancaman Siber

Korelasi positif yang kuat menunjukkan bahwa ketika efektivitas penegakan hukum meningkat, ada peningkatan yang sesuai dalam tingkat keparahan ancaman siber yang dirasakan. Hal ini mendorong dilakukannya pemeriksaan yang lebih mendalam mengenai apakah peningkatan penegakan hukum mengarah pada deteksi yang lebih besar atau eskalasi ancaman siber.

Analisis Regresi

Kedua model regresi menunjukkan dampak signifikan dari penegakan hukum terhadap pengurangan ancaman siber (sig 0.01). Model komprehensif menggarisbawahi pentingnya kerja sama internasional dan pembaruan legislatif, yang berkontribusi pada pemahaman yang lebih menyeluruh sebanyak 62%.

4.2 Temuan Kualitatif

Tema 1: Efektivitas Tindakan Hukum Saat Ini

Temuan: Para peserta menyampaikan berbagai pandangan tentang efektivitas langkah-langkah hukum saat ini, dengan beberapa menyoroti keberhasilan dalam penuntutan dan pencegahan, sementara yang lain menekankan perlunya pembaruan terus-menerus untuk mengimbangi ancaman yang terus berkembang.

Kutipan:

"Kerangka hukum telah memberikan dasar yang kuat, tetapi kita perlu beradaptasi dengan cepat untuk mengatasi taktik baru yang digunakan oleh penjahat siber."

"Penegakan hukum telah membaik, tetapi kompleksitas ancaman siber menuntut pendekatan hukum yang lebih dinamis."

Tema 2: Tantangan dalam Penegakan Hukum

Temuan: Tantangan dalam penegakan hukum diakui, termasuk keterbatasan sumber daya, masalah yurisdiksi internasional, dan kebutuhan akan kolaborasi yang lebih baik antara sektor publik dan swasta.

Kutipan:

"Sumber daya yang terbatas menghambat kemampuan kami untuk menyelidiki dan menuntut penjahat siber secara efektif."

"Masalah lintas batas menyulitkan untuk membawa pelaku ke pengadilan. Kami membutuhkan lebih banyak kolaborasi internasional."

Tema 3: Rekomendasi untuk Perbaikan

Temuan: Para peserta memberikan rekomendasi untuk memperkuat kerangka kerja hukum, termasuk peningkatan kerja sama internasional, pembaruan legislatif secara berkala, dan pembentukan badan keamanan siber terpusat.

Kutipan:

"Kami membutuhkan badan khusus yang hanya berfokus pada keamanan siber, yang menyatukan keahlian dari berbagai sektor."

"Kerja sama internasional adalah kuncinya. Ancaman siber tidak mengenal batas, dan kerangka hukum kita harus mencerminkan kenyataan itu."

4.3 Pembahasan

Efektivitas Kerangka Hukum yang Ada

Tingkat keparahan ancaman siber yang dirasakan selaras dengan peringkat efektivitas, yang mengindikasikan kesadaran kolektif akan tantangan yang ada. Persepsi yang beragam di antara kelompok peserta menyoroti perlunya pendekatan yang disesuaikan untuk mengatasi masalah sektor tertentu.

Korelasi Antara Penegakan Hukum dan Tingkat Keparahan Ancaman Siber

Korelasi positif yang kuat menunjukkan bahwa ketika penegakan hukum meningkat, ada peningkatan yang sesuai dalam tingkat keparahan ancaman siber yang dirasakan. Hal ini mendorong dilakukannya pemeriksaan yang lebih mendalam mengenai apakah peningkatan penegakan hukum mengarah pada deteksi yang lebih besar atau eskalasi ancaman siber.

Wawasan Analisis Regresi

Model regresi menggarisbawahi peran penting penegakan hukum dalam mengurangi ancaman siber. Model komprehensif ini menekankan pentingnya kerja sama internasional dan pembaruan legislatif dalam mencapai pengurangan yang lebih menyeluruh.

Wawasan Kualitatif

Wawasan kualitatif memberikan kedalaman pada temuan kuantitatif. Pandangan peserta tentang tantangan dan rekomendasi sejalan dengan analisis statistik, menyoroti kendala sumber daya, masalah lintas batas, dan kebutuhan untuk adaptasi hukum yang dinamis.

Implikasi untuk Kebijakan dan Praktik

Temuan penelitian ini memiliki implikasi yang signifikan bagi para pembuat kebijakan, praktisi hukum, dan profesional keamanan siber. Rekomendasi utama meliputi:

a. Meningkatkan Kerja Sama Internasional: Memperkuat kolaborasi antar negara untuk mengatasi ancaman siber lintas batas secara efektif.
b. Pembaruan Legislatif yang Dinamis: Menetapkan mekanisme untuk pembaruan kerangka kerja hukum secara berkala guna mengatasi sifat ancaman siber yang terus berkembang.
c. Alokasi Sumber Daya: Mengalokasikan sumber daya secara strategis untuk mengatasi tantangan penegakan hukum dan memastikan efektivitas tindakan hukum.

d. Pembentukan Badan Keamanan Siber: Mempertimbangkan pembentukan badan khusus untuk memusatkan upaya dan keahlian dalam memerangi ancaman siber.

5. KESIMPULAN

Penelitian ini menjelaskan hubungan yang rumit antara hukum dan keamanan siber, menjelaskan efektivitas kerangka hukum yang ada dalam menangani ancaman siber terhadap keamanan nasional di Indonesia. Keragaman demografis responden, termasuk pejabat pemerintah, perwakilan sektor swasta, dan pakar individu, memperkaya kelengkapan dan penerapan temuan ini. Korelasi positif antara efektivitas penegakan hukum yang dirasakan dan tingkat keparahan ancaman siber menggarisbawahi pentingnya langkah-langkah hukum dalam menghadapi tantangan yang terus berkembang. Analisis regresi menegaskan peran penting penegakan hukum sambil menekankan perlunya kolaborasi internasional dan kemampuan beradaptasi legislatif. Wawasan ini memiliki implikasi yang mendalam bagi para pembuat kebijakan dan praktisi, yang mendesak pembaruan legislatif secara teratur, alokasi sumber daya strategis, dan peningkatan kerja sama internasional untuk memperkuat pertahanan siber Indonesia. Seiring dengan perjalanan Indonesia menuju masa depan digital, penelitian ini berfungsi sebagai panduan dasar untuk membentuk kerangka kerja hukum yang tangguh dan adaptif dalam perang yang sedang berlangsung melawan ancaman siber terhadap keamanan nasional.

DAFTAR PUSTAKA

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20.

Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, *29*(5), 554–575.

Dewi, S. (2015). Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia. *Jurnal De Jure*, *15*(2), 23.

Ehrlich, M., Wisniewski, L., Trsek, H., & ... (2017). Automatic mapping of cyber security requirements to support network slicing in software-defined networks. *2017 22nd IEEE …*. https://ieeexplore.ieee.org/abstract/document/8247728/

Gomes, J. F., Iivari, M., Ahokangas, P., & ... (2018). Cyber security business models in 5g. *… Guide to 5G Security*. https://doi.org/10.1002/9781119293071.ch5

Greenleaf, G. (2012). ASEAN's 'New'Data Privacy Laws: Malaysia, the Philippines and Singapore. *Privacy Laws & Business International Report*, *116*, 22–24.

Greenleaf, G. (2017). *ASEAN's Two Speed Data Privacy Laws: Some Race Ahead*.

Jaman, U. B. (2022). Prospek Hak Kekayaan Intelektual (HKI) sebagai Jaminan Utang. *Jurnal Hukum Dan HAM Wara Sains*, *1*(01), 15–20.

Jaman, U. B. (2023). Legal Analysis of The Impact of Industrial Development on The Environment. *The Easta Journal Law and Human Rights*, *1*(03), 87–92.

Jaman, U. B., Nuraeni, A. H., Pitaloka, B. P., & Gadri, K. Z. (2022). Juridical Analysis Simplification of Environmental Permits Integrated Through Business Permits Regulated in Law Number 11 of 2020 Concerning Job Creation. *Libertas Law Journal*, *1*(1), 10–22.

Jaman, U. B., Putri, G. R., & Anzani, T. A. (2021). Urgensi Perlindungan Hukum Terhadap Hak Cipta Karya Digital. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *3*(1), 9–17.

Jaman, U. B., & Zulfikri, A. (2022). Peran serta Masyarakat dalam Pencegahan Kekerasan Seksual dihubungkan dengan UU No. 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual. *Jurnal Hukum Dan HAM Wara Sains*, *1*(01), 1–7.

Juaningsih, I. N., Hidayat, R. N., Aisyah, K. N., & Rusli, D. N. (2021). Rekonsepsi Lembaga Pengawas Terkait Perlindungan Data Pribadi Oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi. *Dalam Jurnal Salam Jurnal Sosial Dan Budaya Syar-I*, *8*(1).

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*.

Lintasarta. (2020). *Ancaman dan Tantangan Keamanan Siber di Industri Kesehatan*. 10 November 2020.

Natamiharja, R., Sabatira, F., Fakih, M., Davey, O. M., & Anam, H. (2022). Patient Rights During the Covid-19 Pandemic: The Dilemma between Data Privacy and Transparency in Indonesia. *The Age of Human Rights Journal*, *19*, 121–136.

Paxy, R., Sinta, A., & Rio, A. (2020). Evaluasi Model Bisnis Pentesting Indonesia Dengan Menggunakan Metode Business Model Canvas. *EProceedings …*, *7*(3), 9463–9470. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/download/14166/13905

Pfeiffer, A., Denk, N., Wernbacher, T., Bezzina, S., Vella, V., & Dingli, A. (2022). Two novel use-cases for non-fungible tokens (NFTs). *European Conference on Cyber Warfare and Security*, *21*(1), 214–221.

Prameswati, V., Sari, N. A., & Nahariyanti, K. Y. (2022). Data Pribadi Sebagai Objek Transaksi di NFT pada Platform Opensea. *Jurnal Civic Hukum*, *7*(1).

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303.

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal*, *5*(1), 143–157.

Shrivastava, U., Song, J., Han, B. T., & Dietzman, D. (2021). Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics*, *148*, 104401.

Trautman, L. J. (2021). Rapid Technological Change and US Entrepreneurial Risk in International Markets: Focus on Data Security, Information Privacy, Bribery and Corruption. *Cap. UL Rev.*, *49*, 67.

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, *1*(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030