Legitimacy: Journal of Law and Islamic Law
Published by CV. Era Digital Nusantara
Volume 1 Issue 3, 2026 ISSN (Online) ***3110-6749***
Journal Homepage: **https://jurnal.erapublikasi.id/index.php/JOLIL**

The Impact of Technological Advancements on Criminal Law Amidst Global Digitalization

Pengaruh Perkembangan Teknologi Terhadap Hukum Pidana Digitalitasasi Global

Elisabeth S. Telussa[1], **Alynne H Matulapelwa**[2] **John D Pasalbessy**[3]
[1-3]Fakultas Hukum, Universitas Kristen Indonesia Maluku, Indonesia

Article Info

Corresponding Author:
Elisabeth S. Telussa
✉elisabethtelussa06@gmail.com

History:
Submitted: 14-12-2025
Revised: 14-01-2026
Accepted: 30-01-2026

Keyword:
UN Cybercrime Convention 2024; Digital Jurisdiction; Artificial Intelligence; Progressive Law; Transnational Crime.

Kata Kunci:
Konvensi Kejahatan Siber PBB 2024; Yurisdiksi Digital; Kecerdasan Buatan; Hukum Progresif; Kejahatan Transnasional.

Copyright © 2026 by Legitimacy: Journal of Law and Islamic Law.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA).

https://doi.org/10.59066/jolil.v1i3.2176

Abstract

This study analyzes the transformative impact of global digitalization, specifically Artificial Intelligence and the Metaverse, on criminal law doctrines. Utilizing a normative-juridical approach, it critically examines the United Nations Convention Against Cybercrime 2024 as a pivotal yet controversial instrument affecting state sovereignty and human rights through expanded passive personality jurisdiction. The research highlights the "jurisdictional creep" phenomenon and the complexities of establishing locus delicti in a borderless cyberspace. Contextualizing these global shifts within Indonesia, the analysis reveals significant vulnerabilities in domestic infrastructure, evidenced by recent ransomware attacks, and a regulatory disconnect between current national statutes and international standards. Consequently, this article advocates for a paradigm shift from rigid territorial positivism toward progressive legal enforcement strategies. It concludes that effective digital sovereignty requires harmonizing cross-border evidence mechanisms and strengthening judicial oversight to balance national security with individual privacy rights within an evolving transnational criminal ecosystem.

Abstrak

Studi ini menganalisis dampak transformatif digitalisasi global, khususnya Kecerdasan Buatan dan Metaverse, terhadap doktrin hukum pidana. Menggunakan pendekatan yuridis-normatif, penelitian ini secara kritis mengkaji Konvensi PBB Melawan Kejahatan Siber 2024 sebagai instrumen krusial namun kontroversial yang memengaruhi kedaulatan negara dan hak asasi manusia melalui perluasan yurisdiksi personalitas pasif. Riset ini menyoroti fenomena "perluasan yurisdiksi" dan kompleksitas penetapan *locus delicti* dalam ruang siber tanpa batas. Mengontekstualisasikan pergeseran global ini di Indonesia, analisis mengungkap kerentanan signifikan pada infrastruktur keamanan domestik, dibuktikan oleh serangan ransomware baru-baru ini, serta kesenjangan regulasi antara undang-undang nasional saat ini dan standar internasional. Konsekuensinya, artikel ini mengadvokasi pergeseran paradigma dari positivisme teritorial yang kaku menuju strategi penegakan hukum progresif. Disimpulkan bahwa kedaulatan digital efektif memerlukan harmonisasi mekanisme pertukaran bukti lintas batas dan penguatan pengawasan yudisial untuk menyeimbangkan keamanan nasional dengan hak privasi individu dalam ekosistem kriminal transnasional yang terus berkembang.

A. PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK) telah mencapai titik puncaknya dalam era revolusi digital, di mana internet bukan lagi sekadar alat komunikasi, melainkan telah menjadi simbol material dari embrio masyarakat global yang merenovasi seluruh sendi kehidupan. Transformasi ini membawa perubahan struktural yang fundamental, menggeser pola interaksi manusia dari struktur masyarakat lokal menuju struktur masyarakat global yang tanpa batas (*borderless*). Dalam realitas baru ini, kehidupan manusia terbelah antara dunia nyata (*real*) dan realitas maya (*virtual*) yang dikenal sebagai *cyberspace*, sebuah lingkungan imajiner di mana setiap individu dapat berinteraksi tanpa hambatan ruang dan waktu melalui jaringan komputer internasional.[1] Kehadiran *cyberspace* ini, sebagaimana diungkapkan oleh Howard Rheingold, memungkinkan setiap orang melakukan aktivitas sosial sehari-hari dengan cara-cara baru yang artifisial, yang pada gilirannya membentuk ruang publik baru (*public sphere*) sesuai dengan teori Habermas.[2]

Namun, kemajuan teknologi yang serba digital ini ibarat pedang bermata dua. Di satu sisi, ia memberikan kontribusi besar bagi kesejahteraan dan kemajuan peradaban, namun di sisi lain, ia menjadi sarana yang sangat efektif bagi perbuatan melawan hukum yang bersifat canggih dan lintas negara. Kejahatan dunia maya (*cybercrime*) kini telah berevolusi menjadi *extraordinary crime*, *serious crime*, dan *transnational crime* yang dilakukan oleh para intelektual dalam lingkup *white collar crime*.[3] Fenomena ini mencakup berbagai bentuk perbuatan hukum baru yang memerlukan adaptasi cepat dalam pembentukan peraturan perundang-undangan sebagai hukum positif. Pertumbuhan aktivitas digital yang eksponensial dalam beberapa dekade terakhir tidak hanya mengancam keamanan siber, tetapi juga stabilitas bisnis, perdagangan, komunitas swasta, hingga lembaga publik.[4]

---

[1] Raodia Raodia, "Space of Flows," in *Encyclopedia of Geography*, vol. 6 (2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2010), 230–239, https://doi.org/10.4135/9781412939591.n1052.

[2] Howard Rheingold, "Daily Life in Cyberspace," in *The Virtual Community* (The MIT Press, 2000), https://doi.org/10.7551/mitpress/7105.003.0005.

[3] Raodia Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (December 30, 2019): 230–239, https://doi.org/10.24252/jurisprudentie.v6i2.11399.

[4] Irma Yurita, M. Kevin Ramadhan, and M. Candra, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (Studi Kasus Phising Sebagai Ancaman Keamanan Digital)," *Jurnal Hukum Legalita* 5, no. 2 (December 23, 2023): 143–55, https://doi.org/10.47637/legalita.v5i2.995.

Pentingnya penelitian ini didasarkan pada fakta bahwa hukum pidana tradisional yang berbasis pada kedaulatan teritorial fisik sering kali gagal merespons karakteristik kejahatan siber yang bersifat lintas batas. Dimensi global dari kejahatan ini memicu konflik yurisdiksi yang kompleks, di mana suatu tindakan kriminal dapat dilakukan oleh pelaku di negara A, menggunakan server di negara B, dan menimbulkan dampak merugikan di negara C.[5] Sejak tahun 1990-an, Perserikatan Bangsa-Bangsa (PBB) telah berupaya menangani masalah ini, namun baru pada akhir tahun 2024 dunia mencapai konsensus bersejarah dengan diadopsinya Konvensi PBB melawan Kejahatan Siber.[6]

Kajian teori dalam artikel ini mencakup berbagai asas hukum internasional, seperti *subjective territoriality*, *objective territoriality*, *nationality*, *passive nationality*, *protective principle*, dan *universality*. Gagasan kritis konseptual yang disajikan berfokus pada bagaimana hukum pidana digitalisasi global harus dirancang untuk mengatasi tantangan penegakan hukum lintas batas, perlindungan data internasional, dan ketentuan pengadilan digital.

Penelitian terdahulu telah memberikan landasan bagi pemahaman kejahatan siber. Donn B. Parker mengidentifikasi kejahatan dunia maya sebagai objek, lingkungan, instrumen, atau simbol kejahatan.[7] Penelitian oleh Gupta & Srivastava (2023) menyoroti pergeseran masyarakat menuju platform digital yang memberikan kenyamanan bagi pelaku pemalsuan kartu ATM dan kredit.[8] Sementara itu, Laufs & Borrion (2022) menganalisis penggunaan teknologi seperti drone dan kamera tubuh dalam kepolisian yang merevolusi penegakan hukum.[9] Namun, terdapat perbedaan signifikan antara penelitian-penelitian tersebut dengan artikel yang sedang ditulis ini. Artikel ini menawarkan analisis yang lebih kontemporer dengan memfokuskan pada adopsi Konvensi PBB tentang Kejahatan Siber tahun 2024 dan munculnya kategori kejahatan masa depan seperti "*metacrime*" di dalam metaverse.

---

[5] Susan W. Brenner, "Cybercrime Jurisdiction," *Crime, Law and Social Change* 46, no. 4–5 (December 14, 2006): 189–206, https://doi.org/10.1007/s10611-007-9063-7.
[6] Tatiana Tropina, "'This Is Not a Human Rights Convention!': The Perils of Overlooking Human Rights in the UN Cybercrime Treaty," *Journal of Cyber Policy* 9, no. 2 (May 3, 2024): 200–220, https://doi.org/10.1080/23738871.2024.2419517.
[7] Donn B. Parker, "Toward a New Framework for Information Security?," in *Computer Security Handbook* (Wiley, 2012), https://doi.org/10.1002/9781118851678.ch3.
[8] Reeta R Gupta and Asha Srivastava, "Impact of Emerging Technology on Recent Criminal Scenario," *IP International Journal of Forensic Medicine and Toxicological Sciences* 8, no. 2 (July 28, 2023): 65–68, https://doi.org/10.18231/j.ijfmts.2023.013.
[9] Julian Laufs and Hervé Borrion, "Technological Innovation in Policing and Crime Prevention: Practitioner Perspectives from London," *International Journal of Police Science & Management* 24, no. 2 (June 10, 2022): 190–209, https://doi.org/10.1177/14613557211064053.

Novelty dari penelitian ini terletak pada analisis mendalam terhadap "*jurisdictional creep*" yang dipicu oleh perluasan *passive personality jurisdiction* dalam konvensi internasional terbaru dan dampaknya terhadap hak asasi manusia serta privasi digital. Selain itu, penelitian ini mengeksplorasi penggunaan Kecerdasan Buatan (AI) dalam investigasi kriminal dan bagaimana hukum pidana harus beradaptasi dari paradigma legal-positivistik menuju paradigma hukum progresif untuk mengatasi kompleksitas kejahatan berbasis algoritma.

Temuan dari penelitian ini secara singkat menunjukkan bahwa meskipun instrumen hukum global telah terbentuk melalui Konvensi PBB 2024, efektivitasnya masih terhambat oleh perbedaan budaya hukum nasional, tantangan teknis dalam atribusi pelaku, dan ketegangan antara keamanan nasional dengan hak privasi individu. Penegakan hukum di Indonesia sendiri masih menunjukkan celah antara regulasi domestik (UU ITE dan UU PDP) dengan standar internasional, terutama dalam hal mekanisme kerja sama data lintas batas dan penanganan serangan ransomware berskala besar yang terus meningkat secara drastis.

2. Perumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Bagaimana pengaruh perkembangan teknologi digital, khususnya Kecerdasan Buatan dan Metaverse, terhadap evolusi doktrin hukum pidana dan munculnya bentuk-bentuk kejahatan baru dalam skala global?
b. Bagaimana tantangan yurisdiksi dan efektivitas kerja sama internasional dalam kerangka Konvensi PBB melawan Kejahatan Siber 2024 dibandingkan dengan instrumen hukum yang sudah ada?
c. Sejauh mana kesiapan regulasi hukum positif Indonesia dalam merespons dinamika ancaman siber transnasional dan bagaimana upaya sinkronisasinya dengan norma hukum internasional?

3. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif, yaitu sebuah proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang sedang dihadapi.[1] Metode ini dilakukan dengan menelaah bahan pustaka atau data sekunder sebagai bahan dasar penelitian melalui studi

dokumen.[10]

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) terhadap berbagai sumber hukum primer dan sekunder. Bahan hukum primer mencakup Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta instrumen internasional seperti Konvensi Budapest dan Konvensi PBB melawan Kejahatan Siber 2024. Bahan hukum sekunder diperoleh dari artikel jurnal ilmiah bereputasi, buku teks, laporan lembaga resmi seperti Badan Siber dan Sandi Negara (BSSN) dan *United Nations Office on Drugs and Crime* (UNODC), serta hasil penelitian hukum terdahulu.

Pendekatan penelitian yang digunakan meliputi pendekatan undang-undang (*statute approach*) untuk menganalisis sinkronisasi antarperaturan, dan pendekatan kasus (*case approach*) dengan menelaah insiden siber signifikan, seperti serangan ransomware pada Pusat Data Nasional (PDN) Indonesia tahun 2024. Teknik analisis yang diterapkan adalah analisis tematik untuk mengidentifikasi tren utama, tantangan, dan perubahan paradigma dalam hukum pidana akibat globalisasi digital. Penelitian ini juga melakukan studi perbandingan hukum (*comparative law studies*) untuk mengeksplorasi perbedaan pendekatan hukum pidana di berbagai yurisdiksi, seperti perbandingan antara sistem perlindungan data di Uni Eropa dan Amerika Serikat. Referensi yang digunakan mencakup literatur hukum pidana siber terbaru dari periode 2020-2025 untuk menjamin aktualitas informasi.

B. PEMBAHASAN

1. Pengaruh Perkembangan Teknologi Terhadap Evolusi Doktrin Hukum Pidana

Inovasi di bidang teknologi informasi yang berbasis pada integrasi antara teknologi komunikasi dan komputer telah melahirkan internet sebagai jaringan global skala dunia. Evolusi ini secara signifikan mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru yang menuntut adaptasi hukum positif. Teknologi informasi saat ini menjadi pedang bermata dua; di satu sisi memberikan kontribusi bagi kesejahteraan, namun di sisi lain menjadi sarana efektif bagi perbuatan melawan hukum yang melintasi batas-batas negara

[10] Nurul Qamar and Farah Syah Rezah, *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal* (Makassar: CV. Social Politic Genius (SIGn), 2020). Hal, 30.

(*borderless*).[11]

Perkembangan teknologi telah mengaburkan batasan yurisdiksi tradisional, mengharuskan sistem peradilan pidana untuk beradaptasi dengan dinamika baru yang melibatkan kejahatan lintas batas. Seiring dengan kemajuan zaman, bentuk kejahatan semakin bervariasi. Munculnya teknologi Kecerdasan Buatan (AI) telah membawa tantangan baru bagi paradigma hukum pidana legal-positivistik. Studi Wisnubroto & Tegnan (2025) menunjukkan bahwa paradigma hukum positif saat ini sering kali tidak memadai dalam menangani sifat dinamis dan kompleks dari kejahatan berbasis AI. AI digunakan baik sebagai alat untuk melakukan kejahatan, seperti pembuatan *deepfakes* untuk penipuan finansial, maupun sebagai objek kejahatan melalui manipulasi algoritma.[12]

Selain AI, munculnya konsep "*metacrime*" di dalam metaverse menandai evolusi terbaru dari kriminalitas digital. *Metacrime* mencakup peluang kriminal unik seperti pelanggaran privasi melalui avatar, pencurian aset virtual, dan tantangan dalam menentukan kewajiban hukum bagi identitas digital atau avatar. Karakteristik metacrime yang imersif dan interaktif mempersulit paradigma kejahatan siber yang sudah ada, terutama dalam hal pembuktian dan penentuan niat jahat (*mens rea*) dalam lingkungan virtual yang terdesentralisasi.[13]

Tabel 1. Pengaruh Perkembangan Teknologi Terhadap Evolusi Doktrin Hukum Pidana

Jenis Teknologi	Dampak pada Kriminologi	Tantangan Hukum Pidana
Internet & Komputer	Globalisasi kejahatan siber tradisional	*Locus delicti* lintas batas, anonimitas pelaku
Kecerdasan Buatan (AI)	Kejahatan berbasis algoritma, deepfakes	Bias algoritma, liabilitas mesin vs manusia
Metaverse	*Metacrime*: pencurian aset virtual, *avatar liability*	Yurisdiksi virtual, hak kepemilikan digital

[11] Izfahany Mahesa Sautaqi, Dewanti Ayu Garnida, and Rifqi Fauzi Effendi, "Dampak Perkembangan Teknologi Terhadap Hukum Sebagai Tantangan Dimensi Baru Keamanan Siber," *De Juncto Delicti: Journal of Law* 3, no. 1 (December 7, 2023): 47–54, https://doi.org/10.35706/djd.v3i1.8048.
[12] Aloysius Wisnubroto and Hilaire Tegnan, "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States," *Journal of Human Rights, Culture and Legal System* 5, no. 2 (September 10, 2025): 630–58, https://doi.org/10.53955/jhcls.v5i2.606.
[13] Milind Tiwari et al., "Confronting Metacrime: Complexities, Enforcement Challenges, and Regulatory Pathways," *Law, Innovation and Technology* 17, no. 1 (January 2, 2025): 159–76, https://doi.org/10.1080/17579961.2025.2469347.

Blockchain/Crypto	Pencucian uang, pendanaan terorisme	Pelacakan aliran dana terenkripsi, volatilitas bukti

Pemanfaatan teknologi dalam investigasi kriminal juga mengalami transformasi. Penegak hukum kini sangat bergantung pada forensik digital untuk membangun kasus, seperti yang terlihat pada penggunaan data GPS, catatan panggilan, dan jejak elektronik lainnya dalam kasus-kasus pembunuhan modern. Namun, penggunaan AI dalam *predictive policing* dan pengambilan keputusan hukum menimbulkan risiko diskriminasi dan bias terhadap kelompok marginal, yang pada akhirnya menantang prinsip keadilan dan hak asasi manusia.[14]

2. Analisis Kontemporer Konvensi PBB Melawan Kejahatan Siber 2024

Tonggak sejarah terpenting dalam hukum pidana digitalitas global baru-baru ini adalah diadopsinya Konvensi PBB melawan Kejahatan Siber pada 24 Desember 2024 melalui resolusi 79/243. Konvensi ini merupakan instrumen hukum global pertama yang mengikat secara hukum dan bertujuan untuk memperkuat kerja sama internasional dalam memerangi ancaman digital. Sebelum adanya konvensi ini, kerangka kerja internasional utama adalah Konvensi Budapest, yang meskipun komprehensif, dianggap kurang memiliki keanggotaan universal karena absennya negara-negara besar seperti Rusia dan China.[15]

Konvensi PBB 2024 mengkriminalisasi berbagai pelanggaran yang bergantung pada komputer (*cyber-dependent*) seperti akses tidak sah dan penyebaran malware, serta pelanggaran yang difasilitasi oleh komputer (*cyber-enabled*). Salah satu aspek fundamental dari konvensi ini adalah upaya standarisasi pertukaran bukti elektronik untuk kejahatan serius lainnya, yang melampaui sekadar kejahatan siber murni.[16]

Namun, konvensi ini tidak luput dari kritik tajam. Para ahli hukum menyoroti adanya fenomena "*jurisdictional creep*", khususnya perluasan *passive personality jurisdiction* dalam Pasal 22(2)(a). Ketentuan ini memberikan wewenang kepada negara untuk mengklaim yurisdiksi atas kejahatan yang dilakukan di mana pun di dunia jika korbannya adalah warga negara mereka. Hal ini dianggap sebagai ancaman terhadap

[14] Dr. Ahmad Hazim Mustafa, "The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence," *Pakistan Journal of Life and Social Sciences (PJLSS)* 22, no. 2 (2024): 9519–35, https://doi.org/10.57239/PJLSS-2024-22.2.00721.
[15] Jonathan Clough, "The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World," *Criminal Law Forum* 23, no. 4 (December 25, 2012): 363–91, https://doi.org/10.1007/s10609-012-9183-3.
[16] Mustafa, "The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence."

kedaulatan negara, hak atas proses hukum yang adil (*due process*), dan hak asasi manusia, karena dapat digunakan oleh negara otoriter untuk menargetkan pembangkang politik secara global.

Tabel 2. Analisis Kontemporer Konvensi PBB Melawan Kejahatan Siber

Fitur Utama Konvensi PBB 2024	**Deskripsi dan Fungsi**	**Kritik dan Tantangan**
Harmonisasi Delik	Menetapkan standar minimum untuk tindak pidana siber global	Definisi yang dianggap terlalu luas dalam beberapa pasal
Jaringan Kontak 24/7	Menyediakan bantuan investigasi lintas batas secara instan	Ketergantungan pada kapasitas teknis domestik yang timpang
Kerja Sama Bukti Digital	Mekanisme berbagi bukti elektronik untuk kejahatan serius	Kurangnya standar perlindungan data pribadi yang seragam
Ekstradisi & MLA	Menggunakan konvensi sebagai dasar hukum bantuan timbal balik	Prinsip *dual criminality* tetap menjadi penghambat operasional

Kritik lain menyatakan bahwa konvensi ini cenderung lambat dibandingkan dengan kecepatan inovasi para penjahat siber. Kelompok kriminal siber dapat menghapus jejak dan berpindah yurisdiksi dalam hitungan jam, sementara mekanisme *Mutual Legal Assistance* (MLA) yang diatur dalam konvensi tetap bersifat birokratis dan memakan waktu lama.[17] Sebagai perbandingan, inisiatif yang lebih lincah seperti *Counter Ransomware Initiative* (CRI) telah terbukti lebih efektif dalam melakukan disrupsi infrastruktur kriminal secara *real-time*, seperti pada kasus penindakan LockBit.[18]

3. Dinamika Yurisdiksi dan Locus Delicti dalam Ruang Siber

Penentuan hukum yang berlaku dan lokasi tindak pidana (*locus delicti*) merupakan tantangan terbesar dalam hukum pidana digitalitas global. Karakteristik *cyberspace* yang melampaui wilayah teritorial negara meniadakan konsep tradisional tentang perbatasan

[17] Muhammad Yudha Prawira and Fatra Alamsyah, "The Implementation of Mutual Legal Assistance between Indonesia and Switzerland Regarding Asset Recovery," *Indonesian Comparative Law Review* 5, no. 2 (May 19, 2023): 58–74, https://doi.org/10.18196/iclr.v5i2.17435.
[18] Tsvetelina J van Benthem and Roxana Radu, "Domestic and International Approaches to Combating Ransomware: Between Contradiction and Coherence," *International Journal of Law and Information Technology* 34 (January 12, 2026), https://doi.org/10.1093/ijlit/eaag004.

fisik. Dalam hukum pidana internasional, terdapat beberapa asas yurisdiksi yang digunakan untuk menjawab tantangan ini:[19]

a. *Subjective Territoriality*: Menekankan tempat perbuatan dilakukan, meskipun penyelesaiannya di negara lain.
b. *Objective Territoriality*: Menekankan pada tempat di mana akibat utama perbuatan itu terjadi dan merugikan negara tersebut.
c. *Nationality*: Jurisdiksi berdasarkan kewarganegaraan pelaku.
d. *Passive Nationality*: Jurisdiksi berdasarkan kewarganegaraan korban.
e. *Protective Principle*: Melindungi kepentingan vital negara dari kejahatan di luar wilayahnya.
f. *Universality*: Hak setiap negara untuk menghukum pelaku kejahatan terhadap kemanusiaan.

Dalam praktiknya, penentuan *locus delicti* di Indonesia menggunakan tiga konsep utama: *locus actus* (lokasi perbuatan pelaku), *locus effectus* (lokasi timbulnya akibat), dan *locus instrumentum* (lokasi alat atau infrastruktur yang digunakan). Sebagai contoh, dalam kasus peretasan terhadap perusahaan Indonesia pada tahun 2024 oleh pelaku yang berada di luar negeri, lokasi perbuatan berada di negara asal pelaku, namun lokasi akibat berada di Indonesia karena kerugian ekonomi dirasakan di sini, sementara lokasi instrumen bisa berada di negara ketiga (misalnya server awan di Singapura).[20]

Berdasarkan Pasal 2 UU ITE, Indonesia menganut prinsip yurisdiksi ekstrateritorial yang memungkinkan hukum Indonesia berlaku bagi setiap orang yang melakukan perbuatan hukum di luar wilayah Indonesia, asalkan perbuatan tersebut memiliki akibat hukum di wilayah Indonesia atau merugikan kepentingan Indonesia. Namun, efektivitas penegakan hukum ini sering kali terbentur oleh "void" atau kekosongan hukum dalam hal kerja sama data lintas batas dan ekstradisi pelaku.[21]

[19] Arthur Simada et al., "Penentuan Locus Delictie Dalam Tindak Pidana Cyber Crime (Merusak Dan Mengganggu Sistem Elektronik Dan Komunikasi Milik Orang Lain)," *Locus Journal of Academic Literature Review* 3, no. 4 (April 29, 2024): 349–61, https://doi.org/10.56128/ljoalr.v3i4.314.
[20] Agustinus Nicholas L Tobing and Annisa Fitria, "Legal Jurisdiction and Place of Occurrence in Transnational Cybercrime: A Normative Analysis of Global Law and Indonesian Telecommunications Regulations," *Awang Long Law Review* 8, no. 2 (January 16, 2026): 530–38, https://doi.org/10.56301/awl.v8i2.1894.
[21] Sigid Suseno et al., "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences* 11, no. 1 (December 31, 2025), https://doi.org/10.1080/23311886.2024.2439543.

4. Realitas Ancaman dan Kesiapan Regulasi di Indonesia

Indonesia merupakan salah satu negara dengan pertumbuhan ekonomi digital tercepat, namun sekaligus menjadi target utama serangan siber di Asia Tenggara. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan angka yang sangat mengkhawatirkan: tercatat 3,64 miliar serangan siber atau anomali lalu lintas data terjadi di Indonesia hanya pada periode Januari hingga Juli 2025. Mayoritas serangan tersebut (83,68%) berbasis malware, diikuti oleh akses tidak sah dan eksploitasi sistem.[22]

Beberapa insiden siber besar baru-baru ini telah mengekspos kerentanan infrastruktur digital nasional:[23]

a. Serangan *Ransomware* PDN (2024): Pusat Data Nasional yang menjadi tulang punggung layanan pemerintah diserang oleh grup "*Brain Cipher*", melumpuhkan 282 instansi pemerintah dan memicu permintaan tebusan sebesar 8 juta USD.
b. Kebocoran Data Bank: Kasus kebocoran data nasabah pada beberapa bank besar di Indonesia (BSI, BRI) telah memicu perlunya audit keamanan siber yang lebih ketat dan penguatan regulasi di sektor perbankan.
c. Fraud Keuangan Digital: Lonjakan penggunaan QRIS diikuti oleh peningkatan penipuan berbasis AI dan *deep-fake* yang mengeksploitasi celah dalam literasi digital masyarakat.

Tabel 4. Statistik Siber Indonesia 2024-2025

Statistik Siber Indonesia 2024-2025	Angka / Data	Sumber Data
Jumlah Serangan Siber (H1 2025)	3,64 Miliar anomali	BSSN
Komposisi Serangan Malware	83,68% dari total serangan	BSSN
Kerugian Ekonomi akibat Cybercrime (2025)	Rp 29,7 Miliar (estimasi)	BSSN / Analisis
Prediksi Kenaikan Fraud Transnasional	70% pada tahun 2025	BSSN [3]
Peringkat Target Serangan Global	Posisi ke-10 di Dunia	Kominfo [11]

[22] Defara Dhanya, "Indonesia's BSSN Records 3.64 Billion Cyberattacks in First Half of 2025," Tempo English, 2025.
[23] Mordor Intelligence, "Indonesia Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)," Mordor Intelligence, 2026, https://www.mordorintelligence.com/industry-reports/indonesia-cybersecurity-market.

Secara regulasi, Indonesia telah memiliki UU ITE (terbaru revisi UU No. 1 Tahun 2024) dan UU Pelindungan Data Pribadi (UU No. 27 Tahun 2022). Namun, tantangan utama tetap pada implementasi dan sinkronisasi dengan standar internasional. UU ITE masih dianggap lebih berorientasi pada penegakan domestik dan kekurangan mekanisme untuk kerja sama internasional yang lincah. Sementara itu, UU PDP masih menghadapi kendala dalam penegakan sanksi terhadap platform yang lalai dalam melindungi data pengguna. Saat ini, pemerintah tengah menggodok Rancangan Undang-Undang Keamanan dan Resiliensi Siber (RUU KKS) untuk memperkuat kapasitas pertahanan siber nasional.

5. Transformasi Menuju Hukum Pidana Progresif dan Digitalitas Global

Dinamika kejahatan di era digital memerlukan pergeseran paradigma dari hukum yang kaku menuju penegakan hukum yang lebih progresif. Prinsip hukum progresif menekankan bahwa hukum harus melayani manusia, bukan sebaliknya, dan harus memiliki fleksibilitas untuk beradaptasi dengan perubahan sosial yang cepat akibat teknologi. Dalam konteks AI, penegakan hukum tidak boleh hanya terpaku pada teks undang-undang yang bersifat statis, melainkan harus mampu melakukan terobosan hukum melalui putusan hakim (*judge-made law*) yang merespons kekosongan regulasi teknis.

Selain itu, tantangan masa depan seperti "*global digitality*" menuntut harmonisasi hukum yang lebih dalam. Terdapat perbedaan budaya hukum yang mencolok antara Amerika Serikat yang melihat privasi sebagai masalah risiko ekonomi, dengan Uni Eropa yang melihatnya sebagai hak asasi manusia fundamental (GDPR). Indonesia, sebagai bagian dari komunitas global, harus mampu menyeimbangkan kebutuhan akan keamanan nasional dengan perlindungan privasi digital warga negaranya agar tidak terjebak dalam model tata kelola digital yang represif.[24]

Peningkatan kapasitas sumber daya manusia juga menjadi faktor krusial. Kekurangan tenaga ahli keamanan siber yang bersertifikat dan fasih berbahasa lokal serta global menghambat kemampuan investigasi lintas batas. Sinergi antara pemerintah, akademisi, dan sektor swasta dalam membangun ekosistem digital yang aman menjadi kunci utama untuk melindungi kedaulatan digital Indonesia di tengah tantangan

[24] Massimo Marelli, "Transferring Personal Data to International Organizations under the GDPR: An Analysis of the Transfer Mechanisms," *International Data Privacy Law* 14, no. 1 (March 22, 2024): 19–36, https://doi.org/10.1093/idpl/ipad022.

globalisasi digital yang tidak terbendung.

C. KESIMPULAN

Evolusi teknologi digital telah mentransformasi hukum pidana dari paradigma teritorial tradisional menuju sistem hukum digitalitas global yang melampaui batas negara melalui instrumen internasional seperti Konvensi PBB 2024. Meskipun instrumen global telah memberikan kerangka kerja baru, tantangan yurisdiksi ekstrateritorial dan risiko pelanggaran hak privasi tetap menjadi isu krusial yang harus dimitigasi melalui pengawasan yudisial yang ketat. Indonesia menghadapi ancaman siber yang sangat masif, sehingga memerlukan sinkronisasi regulasi nasional yang lebih responsif serta pergeseran menuju penegakan hukum progresif guna melindungi kedaulatan digital dan kepentingan warga negara. Sinergi internasional dalam pertukaran bukti elektronik dan penguatan kapasitas teknis forensik menjadi prasyarat mutlak untuk menutup celah yurisdiksi yang selama ini dieksploitasi oleh pelaku kejahatan siber transnasional.

DAFTAR PUSTAKA

Benthem, Tsvetelina J van, and Roxana Radu. "Domestic and International Approaches to Combating Ransomware: Between Contradiction and Coherence." *International Journal of Law and Information Technology* 34 (January 12, 2026). https://doi.org/10.1093/ijlit/eaag004.

Brenner, Susan W. "Cybercrime Jurisdiction." *Crime, Law and Social Change* 46, no. 4–5 (December 14, 2006): 189–206. https://doi.org/10.1007/s10611-007-9063-7.

Clough, Jonathan. "The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World." *Criminal Law Forum* 23, no. 4 (December 25, 2012): 363–91. https://doi.org/10.1007/s10609-012-9183-3.

Dhanya, Defara. "Indonesia's BSSN Records 3.64 Billion Cyberattacks in First Half of 2025." Tempo English, 2025.

Gupta, Reeta R, and Asha Srivastava. "Impact of Emerging Technology on Recent Criminal Scenario." *IP International Journal of Forensic Medicine and Toxicological Sciences* 8, no. 2 (July 28, 2023): 65–68. https://doi.org/10.18231/j.ijfmts.2023.013.

Laufs, Julian, and Hervé Borrion. "Technological Innovation in Policing and Crime Prevention: Practitioner Perspectives from London." *International Journal of Police Science & Management* 24, no. 2 (June 10, 2022): 190–209. https://doi.org/10.1177/14613557211064053.

Mahesa Sautaqi, Izfahany, Dewanti Ayu Garnida, and Rifqi Fauzi Effendi. "Dampak Perkembangan Teknologi Terhadap Hukum Sebagai Tantangan Dimensi Baru Keamanan Siber." *De Juncto Delicti: Journal of Law* 3, no. 1 (December 7, 2023): 47–54. https://doi.org/10.35706/djd.v3i1.8048.

Marelli, Massimo. "Transferring Personal Data to International Organizations under the

GDPR: An Analysis of the Transfer Mechanisms." *International Data Privacy Law* 14, no. 1 (March 22, 2024): 19–36. https://doi.org/10.1093/idpl/ipad022.

Mordor Intelligence. "Indonesia Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)." Mordor Intelligence, 2026. https://www.mordorintelligence.com/industry-reports/indonesia-cybersecurity-market.

Mustafa, Dr. Ahmad Hazim. "The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence." *Pakistan Journal of Life and Social Sciences (PJLSS)* 22, no. 2 (2024): 9519–35. https://doi.org/10.57239/PJLSS-2024-22.2.00721.

Parker, Donn B. "Toward a New Framework for Information Security?" In *Computer Security Handbook*. Wiley, 2012. https://doi.org/10.1002/9781118851678.ch3.

Prawira, Muhammad Yudha, and Fatra Alamsyah. "The Implementation of Mutual Legal Assistance between Indonesia and Switzerland Regarding Asset Recovery." *Indonesian Comparative Law Review* 5, no. 2 (May 19, 2023): 58–74. https://doi.org/10.18196/iclr.v5i2.17435.

Qamar, Nurul, and Farah Syah Rezah. *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. Makassar: CV. Social Politic Genius (SIGn), 2020.

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (December 30, 2019): 230–239. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

———. "Space of Flows." In *Encyclopedia of Geography*, 6:230–239. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2010. https://doi.org/10.4135/9781412939591.n1052.

Rheingold, Howard. "Daily Life in Cyberspace." In *The Virtual Community*. The MIT Press, 2000. https://doi.org/10.7551/mitpress/7105.003.0005.

Simada, Arthur, Syafruddin Kalo, Mohammad Ekaputra, and Jelly Leviza. "Penentuan Locus Delictie Dalam Tindak Pidana Cyber Crime (Merusak Dan Mengganggu Sistem Elektronik Dan Komunikasi Milik Orang Lain)." *Locus Journal of Academic Literature Review* 3, no. 4 (April 29, 2024): 349–61. https://doi.org/10.56128/ljoalr.v3i4.314.

Suseno, Sigid, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita, and Bernadette Aurellia Nathania Tiarma. "Cybercrime in the New Criminal Code in Indonesia." *Cogent Social Sciences* 11, no. 1 (December 31, 2025). https://doi.org/10.1080/23311886.2024.2439543.

Tiwari, Milind, You Zhou, Paul Gilmour, and Ausma Bernot. "Confronting Metacrime: Complexities, Enforcement Challenges, and Regulatory Pathways." *Law, Innovation and Technology* 17, no. 1 (January 2, 2025): 159–76. https://doi.org/10.1080/17579961.2025.2469347.

Tobing, Agustinus Nicholas L, and Annisa Fitria. "Legal Jurisdiction and Place of Occurrence in Transnational Cybercrime: A Normative Analysis of Global Law and Indonesian Telecommunications Regulations." *Awang Long Law Review* 8, no. 2 (January 16, 2026): 530–38. https://doi.org/10.56301/awl.v8i2.1894.

Tropina, Tatiana. "'This Is Not a Human Rights Convention!': The Perils of Overlooking Human Rights in the UN Cybercrime Treaty." *Journal of Cyber Policy* 9, no. 2 (May 3, 2024): 200–220. https://doi.org/10.1080/23738871.2024.2419517.

Wisnubroto, Aloysius, and Hilaire Tegnan. "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States." *Journal of Human Rights, Culture and Legal System* 5, no. 2 (September 10, 2025): 630–58. https://doi.org/10.53955/jhcls.v5i2.606.

Yurita, Irma, M. Kevin Ramadhan, and M. Candra. "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (Studi Kasus Phising Sebagai Ancaman Keamanan Digital)." *Jurnal Hukum Legalita* 5, no. 2 (December 23, 2023): 143–55. https://doi.org/10.47637/legalita.v5i2.995.