Equality : Journal of Law and Justice
Vol. 1, No. 2, November, 2024, hlm. 221-241

Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia

Criminal Policy in Handling Cyber in the Digital Era

Muhammad Arafat[1], Alexander Tito Enggar Wirasto[2]
E-mail: Muh.Arafat1@gmail.com
[1]Universitas Islam Indonesia
[2]Universitas Atma Jaya Yogyakarta

Info Artikel
|Submitted: 7 November 2024**|Revised**:27 November 2024**|Accepted**: 29 November 2024
How to cite: Muhammad Arafat dan Alexander Tito Enggar Wirasto , "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia", *Equality : Journal of Law and Justice*, Vol. 1 No. 2, November, 2024, hlm. 221-241.

ABSTRACT

Digital technology in Indonesia has significantly impacted sectors such as government, finance, education, and healthcare, offering numerous benefits. However, it has also led to increased cybercrime, including hacking, digital fraud, identity theft, and ransomware, posing threats to national security and public welfare. Regulations like the ITE and PDP Laws have been implemented, yet challenges persist in enforcement and technological adaptation. Indonesia faces challenges in cyber law enforcement, including insufficient technical capacity among law enforcement officers. This study employs a qualitative descriptive approach with an exploratory focus. Data were collected from legal documents, government reports, case studies, journal articles, and academic literature. Thematic analysis was used to identify patterns, challenges, and the effectiveness of cybercrime policies. The findings reveal that Indonesia's cybersecurity policies need reinforcement, particularly in implementation, public education, and technological adaptation. Examples from the United States and the European Union highlight that collaboration between governments and the private sector, stringent data protection regulations, and public education campaigns significantly enhance resilience against cyber threats. This study recommends strengthening the ITE and PDP Laws, promoting digital literacy among the public, enhancing law enforcement capacities, fostering international collaboration, and establishing cyber information-sharing networks to create a robust, effective, and adaptive digital security ecosystem for Indonesia.

Keyword: *Cybercrime, Indonesia, criminal policy, cybersecurity, digital identity.*

ABSTRAK

Perkembangan teknologi digital di Indonesia telah memberikan banyak manfaat dalam berbagai sektor seperti pemerintahan, keuangan, pendidikan, dan kesehatan. Namun, kemajuan ini juga diiringi dengan peningkatan kejahatan siber, seperti peretasan, penipuan digital, pencurian identitas, dan ransomware, yang mengancam keamanan nasional dan kesejahteraan masyarakat. Regulasi seperti UU ITE dan UU PDP telah diterapkan, tetapi tantangan dalam implementasi dan adaptasi terhadap dinamika teknologi tetap signifikan. Indonesia menghadapi kesenjangan dalam penegakan hukum siber, termasuk kurangnya kapasitas teknis aparat hukum, rendahnya kesadaran masyarakat tentang keamanan digital, serta keterbatasan kerjasama internasional untuk menangani kejahatan siber lintas batas. Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan eksploratif. Data diperoleh dari dokumen hukum, laporan pemerintah, studi kasus, artikel jurnal, dan literatur akademik. Analisis dilakukan menggunakan metode tematik untuk mengidentifikasi pola, tantangan, dan efektivitas kebijakan kriminal terkait kejahatan siber. Studi ini menunjukkan bahwa kebijakan siber di Indonesia memerlukan penguatan, terutama dalam hal implementasi, edukasi publik, dan adaptasi teknologi. Contoh dari Amerika Serikat dan Uni Eropa menunjukkan bahwa kolaborasi antara pemerintah dan sektor swasta, regulasi perlindungan data yang ketat, dan kampanye edukasi dapat meningkatkan ketahanan terhadap ancaman siber.

Penelitian ini menyarankan penguatan UU ITE dan UU PDP, literasi digital bagi masyarakat, peningkatan kompetensi aparat hukum, kerjasama internasional, serta pembentukan jaringan pertukaran informasi siber untuk menciptakan ekosistem keamanan digital yang tangguh, efektif, dan responsif terhadap perkembangan teknologi.
Kata Kunci: *Kejahatan Siber, Indonesia, kebijakan kriminal, keamanan siber, identitas digital.*

A. Pendahuluan

Kemajuan teknologi di era digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk di Indonesia. Di satu sisi, perkembangan ini memberikan aksesibilitas dan efisiensi yang tinggi bagi masyarakat, tetapi di sisi lain, ancaman kejahatan siber juga meningkat seiring dengan kemajuan tersebut. Kejahatan siber, seperti pencurian identitas, peretasan, dan penipuan online, semakin sering terjadi, menimbulkan ancaman terhadap keamanan digital dan kesejahteraan publik. Penanganan ancaman ini membutuhkan kebijakan kriminal yang dapat mengikuti dinamika teknologi siber yang terus berkembang. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), lebih dari 800 juta serangan siber tercatat pada tahun 2022 di Indonesia. Sebagian besar serangan ini menargetkan sektor pemerintahan, keuangan, dan infrastruktur publik yang strategis. Selain itu, tren serangan siber global memperkirakan kerugian ekonomi akibat kejahatan ini mencapai $6 triliun pada tahun 2023, menjadikan Indonesia salah satu target utama di kawasan Asia Tenggara.[1]

Dalam konteks Indonesia, serangan siber telah mempengaruhi berbagai sektor, termasuk pemerintahan, keuangan, pendidikan, dan kesehatan. Hal ini menimbulkan tantangan besar bagi pemerintah untuk merumuskan kebijakan kriminal yang dapat mengatasi masalah kejahatan siber secara efektif. Sebagai respons terhadap meningkatnya ancaman ini, pemerintah Indonesia telah mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Pelindungan Data Pribadi (UU PDP). Namun, implementasi kedua regulasi ini menghadapi berbagai kendala, seperti kurangnya harmonisasi dengan kerangka hukum internasional, rendahnya literasi digital, serta keterbatasan sumber daya teknis yang dimiliki aparat penegak hukum. Permasalahan ini menunjukkan pentingnya kajian lebih lanjut untuk memperkuat kebijakan kriminal dalam menghadapi kejahatan siber di Indonesia. [2]

[1]Cecelia Horan And Hossein Saiedian, 'Cyber Crime Investigation: Landscape, Challenges, And Future Research Directions', Journal Of Cybersecurity And Privacy 1, No. 4 (1 December 2021): 580–96, Https://Doi.Org/10.3390/Jcp1040029.

[2]Mohammad Fadil Imran, 'Preventing And Combating Cybercrime In Indonesia', International Journal Of Cyber Criminology 17, No. 1 (2023): 223–35, Https://Doi.Org/Doi:10.5281/Zenodo.4766614; Radita Setiawan And Muhammad Okky Arista, 'Efektivitas Undang-Undang Informasi Dan Transaksi

Salah satu tantangan utama dalam menangani kejahatan siber di Indonesia adalah sifatnya yang lintas batas, yang mengaburkan yurisdiksi hukum tradisional. Kejahatan siber sering kali dilakukan oleh pelaku yang berada di luar negeri, sehingga sulit untuk menentukan jurisdiksi dan menuntut pelaku. Di tingkat internasional, negara-negara maju seperti Amerika Serikat dan Uni Eropa telah mengadopsi kebijakan keamanan siber yang komprehensif. Contohnya adalah *Cybersecurity Information Sharing Act* (CISA) di Amerika Serikat dan *General Data Protection Regulation* (GDPR) di Uni Eropa, yang memberikan perlindungan data secara ketat dan mendorong kerja sama antarinstansi. Indonesia dapat mengambil pembelajaran dari praktik terbaik ini untuk memperkuat sistem keamanannya, oleh sebab itu hal ini mempertegas pentingnya kerjasama internasional dalam menanggulangi kejahatan siber dan meningkatkan keamanan siber secara global.

Ancaman siber di Indonesia juga diperburuk oleh kurangnya kesadaran publik mengenai pentingnya keamanan digital dan praktik perlindungan data pribadi. Banyak individu dan organisasi yang masih belum mengimplementasikan protokol keamanan siber yang memadai, sehingga rentan terhadap serangan siber. Kesadaran dan edukasi mengenai pentingnya keamanan siber merupakan aspek yang krusial dalam menekan angka kejahatan siber dan menjaga kesejahteraan masyarakat di dunia maya.[3]

Meskipun berbagai kebijakan telah diterapkan, tantangan utama dalam penanganan kejahatan siber di Indonesia mencakup rendahnya literasi digital masyarakat, keterbatasan kapasitas teknis aparat hukum, dan sulitnya menangani kasus yang bersifat lintas batas. Oleh karena itu, penelitian ini penting untuk memberikan solusi strategis dalam memperkuat ekosistem keamanan siber, yang tidak hanya mencakup aspek hukum tetapi juga literasi digital dan kerja sama internasional.

Perbandingan dengan kebijakan kriminal di negara lain juga akan menjadi bagian penting dari penelitian ini. Studi ini akan melihat bagaimana negara-negara maju, seperti Amerika Serikat dan Uni Eropa, menangani ancaman siber dan bagaimana Indonesia dapat mengadopsi praktik-praktik terbaik dari negara-negara tersebut. Dengan demikian, penelitian ini akan membantu pemerintah Indonesia merumuskan kebijakan yang lebih komprehensif dalam menangani kejahatan siber.[4]

Elektronik Di Indonesia Dalam Aspek Hukum Pidana', Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan 2, No. 2 (2013): 139–46, Https://Doi.Org/Https://Doi.Org/10.20961/Recidive.V2i2.32324.

[3]Farah Diba Tanzilla, Margaretha Hanita, And Bondan Widiawan, 'Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law', International Journal Of Progressive Sciences And Technologies (Ijpsat 40, No. 2 (2023): 164–70.

[4]P. Hüsch And J. Sullivan, 'Global Approaches To Cyber Policy, Legislation And Regulation', The Royal United Services Institute For Defence And Security Studies, 26 April 2023,

Tantangan utama dalam penegakan hukum terkait kejahatan siber adalah dinamika teknologi yang selalu berubah. Kejahatan siber menjadi semakin canggih, sementara kerangka hukum yang ada sering kali tidak mampu mengimbangi kecepatan perkembangan teknologi. Ini menuntut pemerintah untuk selalu meng-update kebijakan kriminal agar relevan dengan situasi terkini.

Selain aspek hukum, penelitian ini juga akan mengeksplorasi peran kerjasama antarinstansi dalam menanggulangi ancaman siber. Penanganan kejahatan siber tidak hanya menjadi tanggung jawab penegak hukum, tetapi juga melibatkan sektor lain, seperti industri teknologi dan masyarakat sipil. Kolaborasi ini penting untuk menciptakan ekosistem keamanan siber yang kuat dan resilient.

Dalam penelitian sebelumnya, yaitu artikel karya Afifah Rizqy Widianingrum berjudul "Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital"[5] mengkaji tantangan dan implementasi kebijakan siber di Indonesia dengan pendekatan sosiologi hukum, menyoroti aktivitas seperti penipuan online, peretasan, pencurian identitas, dan eksploitasi data pribadi yang semakin kompleks seiring perkembangan teknologi. Dengan UU ITE sebagai landasan utama, penelitian ini menekankan pentingnya koordinasi lintas lembaga, seperti Kepolisian Republik Indonesia dan Badan Siber dan Sandi Negara (BSSN), yang diperkuat oleh studi kasus pencurian data pribadi tahun 2022 untuk mengilustrasikan kebutuhan akan kapasitas teknis dan regulasi yang adaptif. Namun, artikel ini berfokus pada aspek lokal dengan identifikasi tantangan seperti literasi digital yang rendah, perkembangan teknologi yang cepat, serta kurangnya sumber daya teknis. Sebaliknya, penelitian yang akan akan dilakukan oleh penulis mencakup analisis yang lebih luas dengan membandingkan model kebijakan internasional, seperti Cybersecurity Information Sharing Act (CISA) di Amerika Serikat dan General Data Protection Regulation (GDPR) di Uni Eropa, serta menyoroti pentingnya kolaborasi internasional, edukasi publik, dan penguatan regulasi untuk menciptakan ekosistem keamanan siber yang lebih tangguh. Dengan demikian, artikel Penulis melengkapi pendekatan Afifah melalui perspektif global yang memberikan dimensi strategis terhadap pembaruan kebijakan siber di Indonesia.

Penelitian lainnya yang dilakukan oleh Budi Kristian Bivanda Putra berjudul "Kebijakan Aplikasi Tindak Pidana Siber di Indonesia"[6] mengkaji implementasi kebijakan hukum dalam menanggulangi kejahatan siber di Indonesia melalui

---

Https://Www.Rusi.Org/Explore-Our-Research/Publications/Special-Resources/Global-Approaches-Cyber-Policy-Legislation-And-Regulation.

[5]Afifah Rizqy Widianingrum, 'Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital', Journal Iuris Scientia 2, no. 2 (27 July 2024): 90–102, https://doi.org/10.62263/jis.v2i2.40.

[6]Budi Kristian Bivanda Putra, 'Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia', Pamulang Law Review 1, no. 1 (15 July 2019): 1, https://doi.org/10.32493/palrev.v1i1.2842.

pendekatan yuridis normatif, dengan fokus pada tantangan domestik. Artikel ini menyoroti bahwa meskipun UU ITE telah menjadi kerangka hukum utama, penegakan hukum masih menghadapi berbagai hambatan, seperti kelemahan substansi hukum, keterbatasan sarana dan fasilitas, rendahnya kompetensi aparat penegak hukum, serta kurangnya kesadaran masyarakat akan pentingnya keamanan digital. Solusi yang diusulkan meliputi pelatihan teknis bagi aparat hukum, kerjasama internasional, kolaborasi dengan penyedia layanan internet (ISP), dan pembentukan satuan tugas khusus untuk menangani kasus siber. Sebaliknya, penelitian yang akan akan dilakukan oleh penulis mencakup analisis yang lebih luas dengan membandingkan praktik terbaik internasional, seperti Cybersecurity Information Sharing Act (CISA) dari Amerika Serikat dan General Data Protection Regulation (GDPR) dari Uni Eropa, guna memberikan perspektif komparatif. Selain itu, artikel Penulis menekankan pentingnya kolaborasi lintas sektor, literasi digital publik, serta penguatan regulasi berbasis pembelajaran global, menjadikannya lebih strategis dan holistik dibandingkan pendekatan nasional yang diambil oleh Budi. Dengan kombinasi perspektif lokal dan global, artikel Penulis menawarkan rekomendasi yang lebih sistematis untuk membangun ekosistem keamanan siber yang tangguh di Indonesia.

Terdapat juga penelitian yang dilakukan oleh Dwi Nurahman berjudul "Kebijakan Penegakan Hukum Cybercrime dan Pembuktian Yuridis dalam Sistem Hukum Pidana Nasional"[7] mengulas kebijakan penegakan hukum cybercrime di Indonesia dengan pendekatan normatif, menyoroti pembuktian kejahatan siber melalui UU ITE dan *Convention on Cybercrime* 2001. Artikel ini mengidentifikasi tantangan seperti kurangnya harmonisasi yurisdiksi internasional dan keterbatasan sistem pembuktian digital, serta merekomendasikan pendekatan integral yang mencakup langkah penal dan non-penal, seperti modernisasi sistem hukum, peningkatan kapasitas aparat hukum, harmonisasi hukum internasional, dan edukasi masyarakat. Solusi ini menekankan pentingnya kerja sama lintas negara untuk menangani kejahatan siber yang bersifat lintas batas. Berbeda dengan artikel Nurahman yang berfokus pada aspek teknis pembuktian dan kebijakan domestik, artikel Penulis menawarkan pendekatan yang lebih luas dan strategis dengan membandingkan kebijakan internasional seperti Cybersecurity Information Sharing Act (CISA) dari Amerika Serikat dan General Data Protection Regulation (GDPR) dari Uni Eropa. Penulis juga mengintegrasikan rekomendasi praktis seperti literasi digital publik, penguatan regulasi, dan pembentukan jaringan pertukaran informasi siber, memberikan dimensi global dan lintas sektor yang memperkuat

[7]Dwi Nurahman, 'Kebijakan Penegakan Hukum Cybercrime Dan Pembuktian Yuridis Dalam Sistem Hukum Pidana Nasional', KeadilaN Jurnal Fakultas Hukum Universitas Tulang Bawang 17, no. 2 (1 January 2019), https://doi.org/10.37090/keadilan.v17i2.270.

kerangka kebijakan siber di Indonesia. Novelty artikel Penulis terletak pada integrasi pengalaman global dan pendekatan komprehensif berbasis lintas sektor, yang tidak hanya mencakup aspek teknis tetapi juga strategi kolaboratif untuk membangun ekosistem keamanan siber yang tangguh dan responsif terhadap tantangan era digital.

Penelitian ini bertujuan untuk menganalisis efektivitas kebijakan kriminal Indonesia dalam menangani kejahatan siber dan mengidentifikasi kesenjangan dalam regulasi yang ada. Dengan menganalisis kasus-kasus kejahatan siber di Indonesia, penelitian ini akan memberikan pemahaman yang lebih mendalam tentang tantangan yang dihadapi dalam implementasi kebijakan siber dan rekomendasi yang dapat memperkuat kebijakan kriminal di era digital. Tujuan akhir dari penelitian ini adalah memberikan wawasan bagi pemerintah dalam mengembangkan kebijakan kriminal yang adaptif terhadap perubahan teknologi.

B. Metode Penelitian

Metode penelitian ini menggunakan pendekatan deskriptif kualitatif yang bertujuan untuk memahami efektivitas kebijakan kriminal dalam menangani kejahatan siber di Indonesia secara mendalam. Penelitian ini bersifat eksploratif dan difokuskan pada studi kasus yang mengkaji penerapan kebijakan kriminal dalam merespons kejahatan siber, serta mengidentifikasi kesenjangan yang ada dalam regulasi tersebut. Sumber data dalam penelitian ini diperoleh dari berbagai data sekunder, terutama dokumen resmi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), peraturan terkait, laporan pemerintah, serta dokumen kebijakan lainnya yang mendukung analisis. Selain itu, artikel jurnal, literatur akademik, dan studi kasus yang relevan turut digunakan untuk memberikan perspektif yang lebih luas mengenai penerapan kebijakan siber. Pengumpulan data dilakukan dengan teknik studi dokumen yang sistematis, yang bertujuan untuk mengidentifikasi pola, tantangan, dan praktik yang efektif maupun kurang efektif dalam penegakan hukum siber di Indonesia. Analisis data dilakukan dengan metode analisis tematik, di mana dokumen dan data yang terkumpul dikaji secara mendalam untuk mengidentifikasi tema utama yang terkait dengan jenis kejahatan siber, tantangan penegakan hukum, dan efektivitas kebijakan yang ada. Hasil analisis ini diharapkan dapat mengungkap pola, temuan kunci, serta kesenjangan kebijakan yang ada, sehingga dapat memberikan rekomendasi bagi perbaikan dan penguatan kebijakan kriminal di era digital. Dengan pendekatan ini, penelitian bertujuan menghasilkan wawasan komprehensif yang relevan bagi pengembangan kebijakan kriminal dalam menghadapi kejahatan siber di Indonesia.

C. Hasil dan Pembahasan

Penelitian ini mengidentifikasi bahwa kejahatan siber di Indonesia mencakup berbagai bentuk, antara lain:

1. Hacking

Informasi telah menjadi komoditas penting di era digital, namun tingginya nilai strategisnya sering kali membuatnya menjadi target utama kejahatan siber, termasuk peretasan (hacking). Peretasan, yang dilakukan oleh hacker untuk mengakses sistem komputer tanpa izin, dapat bertujuan untuk mencuri data sensitif atau merusak sistem.[8] Di Indonesia, dengan 76,3% penduduk menjadi pengguna internet pada tahun 2022, ancaman peretasan meningkat signifikan, menjadikan Indonesia negara ketiga dengan kasus kebocoran data terbanyak di dunia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur peretasan dalam Pasal 30, yang menetapkan ancaman pidana penjara hingga tujuh tahun dan/atau denda hingga Rp700 juta. Meskipun sudah ada regulasi, ancaman hacking tetap menjadi isu serius yang memerlukan perhatian pemerintah untuk melindungi masyarakat dan menjaga pertahanan negara dari risiko keamanan siber yang terus berkembang.[9]

2. Penipuan Digital (*Cyber Fraud*)

Maraknya perkembangan teknologi di era digital telah meningkatkan berbagai modus penipuan digital (*cyber fraud*), seperti kasus yang ditangani Direktorat Tindak Pidana Siber (*Dittipidsiber*) Bareskrim Polri pada Juni 2024. Dalam kasus ini, tersangka berinisial ZS, bagian dari jaringan internasional, menipu 823 korban di Indonesia melalui modus lowongan kerja palsu dengan total kerugian mencapai Rp59 miliar sejak 2022. Berdasarkan data Kominfo, terdapat 572 ribu aduan penipuan online sejak 2017 hingga September 2024, dengan kategori penipuan jual beli online menjadi yang tertinggi. Penipuan digital diatur dalam Pasal 28 Ayat (1) UU ITE, dengan ancaman pidana hingga enam tahun penjara atau denda maksimal Rp1 miliar, sementara penipuan dengan dampak lebih serius dapat dikenakan Pasal 36 dengan ancaman hingga 12 tahun penjara atau denda Rp12 miliar. Regulasi ini menunjukkan pentingnya pengawasan dan penegakan hukum yang lebih kuat untuk melindungi masyarakat dari kejahatan siber.[10]

---

[8]Benny Cahyadi Et Al., 'Hacker Anak Dalam Perspektif Teori Differential Association: Studi Kasus Peretasan Situs Pengadilan Negeri Kabupaten Konawe', Ikraith-Humaniora 8, No. 1 (March 2024): 329–40, Https://Doi.Org/Https://Doi.Org/10.37817/Ikraith-Humaniora.V8i1.

[9]Abdul Razzaq Et Al., 'Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator)', Global Political Studies Journal 6 (2022), Https://Doi.Org/Doi10.34010/Gpsjournal.V6i1.

[10]Rahel Narda Chaterine And Dani Prabowo, 'Bareskrim Tangkap Buron Kasus Penipuan Ratusan Wni Modus Lowongan Kerja', Kompas.Com, July 2024,

3. Cyberbullying

Bullying, menurut Barbara Coloroso dalam bukunya Stop Bullying, adalah bentuk intimidasi yang dilakukan berulang kali oleh pihak yang lebih kuat terhadap yang lebih lemah, baik secara fisik maupun emosional, dan sering kali melibatkan ketidakseimbangan kekuasaan. Perilaku ini mencakup pelecehan verbal, kekerasan fisik, atau pemaksaan yang dapat didasari oleh ras, agama, atau status sosial.[11] Dalam konteks hukum Indonesia, pencemaran nama baik dan penghinaan diatur dalam Pasal 310, 311, dan 315 KUHP, dengan ancaman pidana mulai dari 9 bulan hingga 4 tahun penjara, tergantung pada tingkat pelanggarannya. UU ITE melalui Pasal 27 Ayat (3) juga mengatur penghinaan melalui media elektronik, yang harus merujuk pada ketentuan KUHP dan memerlukan aduan langsung dari korban sebagai delik aduan absolut. Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008 mempertegas bahwa penghinaan ringan tidak dapat dijerat melalui UU ITE, dan muatan penghinaan elektronik hanya dapat diproses jika dilakukan terhadap individu perseorangan dengan identitas yang jelas. Hal ini menegaskan pentingnya perlindungan hukum terhadap kehormatan individu, baik di ruang fisik maupun digital.[12]

4. Kejahatan terkait Identitas Digital

Kejahatan identitas digital semakin marak di Indonesia seiring meningkatnya penggunaan teknologi dan data pribadi secara online. Kejahatan ini melibatkan pencurian atau penyalahgunaan informasi pribadi, seperti NIK, nomor kartu kredit, dan akun media sosial, untuk tujuan yang merugikan korban. Contohnya adalah kasus Renaldy Bosito, di mana NIK-nya disalahgunakan untuk pengajuan pinjaman tanpa sepengetahuannya, menyoroti kerentanan data pribadi di Indonesia. Penyebab utama maraknya kejahatan ini adalah rendahnya kesadaran masyarakat dalam melindungi data pribadi, seperti penggunaan kata sandi yang lemah dan kurangnya kewaspadaan terhadap phishing. Selain itu, beberapa perusahaan masih gagal menerapkan protokol keamanan yang memadai, sehingga data pelanggan rentan terhadap kebocoran. Pemerintah Indonesia merespons dengan mengesahkan UU PDP tahun 2022, yang mulai berlaku penuh pada Oktober 2024, untuk memberikan perlindungan hukum terhadap privasi warga. Namun, tantangan implementasi regulasi tetap signifikan, sehingga diperlukan edukasi publik, peningkatan standar keamanan

Https://Nasional.Kompas.Com/Read/2024/07/19/16055431/Bareskrim-Tangkap-Buron-Kasus-Penipuan-Ratusan-Wni-Modus-Lowongan-Kerja.

[11]Barbara Coloroso And Santi Indra Astuti, Stop Bullying: Memutuskan Rantai Kekerasan Anak Dari Prasekolah Hingga Smu (Jakarta: Serambi Ilmu Semesta, 2007).

[12]Muhammad Dani Ihkam And I Gusti Ngurah Parwata, 'Tindak Pidana Cyber Bullying Dalam Perspektif Hukum Pidana Di Indonesia', Jurnal Kertha Wicara, Vol. 9, N.D.

perusahaan, dan penegakan hukum yang efektif untuk memitigasi kejahatan identitas digital.[13]

5. Malware dan Ransomware

Malware, termasuk ransomware, adalah perangkat lunak berbahaya yang dirancang untuk merusak, mencuri, atau mengganggu sistem komputer. Ransomware mengenkripsi data korban dan meminta tebusan dalam bentuk mata uang kripto untuk memulihkan akses, namun pembayaran sering kali tidak menjamin pemulihan data.[14] Di Indonesia, serangan ransomware meningkat signifikan, menargetkan sektor pemerintah, swasta, dan layanan publik, seperti serangan pada Pusat Data Nasional (PDN) pada Juni 2024, yang mengganggu layanan imigrasi dan bandara. Pemerintah telah merespons ancaman ini melalui penguatan Badan Siber dan Sandi Negara (BSSN), kerja sama internasional, serta regulasi seperti UU ITE dan UU PDP.[15] Namun, peningkatan kesadaran publik tetap penting melalui edukasi keamanan siber, seperti penggunaan kata sandi yang kuat, waspada terhadap phishing, dan pembaruan perangkat lunak secara rutin. Kolaborasi antara pemerintah dan sektor swasta juga diperlukan untuk memastikan standar keamanan yang tinggi dalam produk dan layanan teknologi. Tanpa kebijakan yang adaptif dan edukasi yang berkelanjutan, serangan ini dapat terus merugikan stabilitas digital nasional.[16]

Menurut data dari Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami 976.429.996 anomali trafik atau serangan siber sepanjang tahun 2022, dengan aktivitas malware sebagai anomali terbanyak.[17] Sektor pemerintahan, keuangan, dan infrastruktur publik menjadi target utama serangan ini. Selain itu, literasi digital masyarakat Indonesia masih tergolong rendah. Survei Status Literasi Digital Indonesia 2022 menunjukkan bahwa indeks literasi digital nasional berada pada

[13]Yedija Otniel Purba And Agus Mauluddin, 'Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online', Jcic: Jurnal Cic Lembaga Riset Dan Konsultan Sosial-Issn 5, No. 2 (2023): 55–66, Https://Doi.Org/10.51486/Jbo.V5i2.113.

[14]Gavin Hull, Henna John, And Budi Arief, 'Ransomware Deployment Methods And Analysis: Views From A Predictive Model And Human Responses', Crime Science 8, No. 1 (12 December 2019): 2, Https://Doi.Org/10.1186/S40163-019-0097-9.

[15]Reuters, 'Cyber Attack Compromised Indonesia Data Centre, Ransom Sought', Reuters.Com, 24 June 2024, Https://Www.Reuters.Com/Technology/Cybersecurity/Cyber-Attack-Compromised-Indonesia-Data-Centre-Ransom-Sought-Reports-Antara-2024-06-24

[16]Frank Cremer Et Al., 'Cyber Risk And Cybersecurity: A Systematic Review Of Data Availability', The Geneva Papers On Risk And Insurance - Issues And Practice 47, No. 3 (17 July 2022): 698–736, Https://Doi.Org/10.1057/S41288-022-00266-6.

[17]Livia Kristianti, 'BSSN Ungkap Serangan Keamanan Siber Di 2022 Turun Dibanding 2021', Antaranews.com, 2023, https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021.

skor 3,54 dari skala 1-5, yang dikategorikan sebagai "sedang".[18] Hal ini mengindikasikan bahwa banyak individu belum memahami cara melindungi data pribadi secara efektif.

Implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai kerangka hukum utama dalam menangani kejahatan siber menghadapi berbagai tantangan yang kompleks. Salah satu hambatan utama adalah keterbatasan dalam penegakan hukum, terutama dalam menangani kejahatan lintas batas yang sering melibatkan teknologi canggih seperti ransomware. Kurangnya harmonisasi yurisdiksi internasional menjadi kendala signifikan dalam menangani kasus yang melibatkan pelaku di luar negeri. Selain itu, sistem pembuktian digital di Indonesia masih terbatas, sehingga memperumit proses hukum terhadap pelaku kejahatan siber. Kondisi ini menunjukkan perlunya pendekatan komprehensif dalam penanganan kejahatan siber, termasuk peningkatan literasi digital masyarakat, penguatan kapasitas penegak hukum, serta kerja sama internasional yang lebih erat untuk menciptakan ekosistem hukum yang responsif.

Sebagai makhluk dinamis, manusia senantiasa beradaptasi dengan perkembangan zaman, termasuk kemajuan teknologi komunikasi yang terus berkembang. Teknologi modern telah membawa berbagai manfaat positif, tetapi juga memunculkan tantangan baru yang membutuhkan respons hukum yang cepat dan relevan. Sebagai negara hukum, Indonesia menegaskan dalam Pasal 1 Ayat (3) UUD 1945 bahwa setiap tindakan harus sesuai dengan peraturan perundang-undangan yang berlaku. Prinsip ubi societas ibi ius menggarisbawahi bahwa hukum harus mengikuti dinamika masyarakat. Dengan pesatnya perkembangan teknologi informasi, pemerintah Indonesia merespons dengan mengesahkan UU ITE pada tahun 2008 sebagai upaya untuk menjaga keteraturan di tengah kemajuan digital.

Dalam perjalanannya, UU ITE mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 untuk menyesuaikan dengan kebutuhan zaman. Perubahan tersebut mencakup berbagai hal, seperti penegasan keberadaan informasi elektronik dalam Pasal 5, penghapusan informasi elektronik yang tidak relevan dalam Pasal 26, serta pengaturan tata cara intersepsi dalam Pasal 31. Pemerintah juga memperluas perannya dalam mencegah penyebaran informasi terlarang melalui Pasal 40, memperkuat mekanisme penyidikan dalam Pasal 43, serta menambah penjelasan terkait Pasal 27 agar lebih harmonis dengan sistem hukum pidana di Indonesia. Revisi ini bertujuan untuk menjadikan UU ITE lebih efektif dalam menjawab tantangan kejahatan siber yang semakin kompleks dan menjaga

[18]Pratiwi Agustini, 'Indeks Literasi Digital Indonesia Kembali Meningkat Tahun 2022', Kominfo, 2023, https://aptika.kominfo.go.id/2023/02/indeks-literasi-digital-indonesia-kembali-meningkat-tahun-2022/.

keamanan digital di Indonesia. Melalui kerangka hukum yang adaptif dan kolaborasi lintas sektor, Indonesia diharapkan dapat menciptakan sistem hukum yang mampu mengakomodasi perkembangan teknologi dan melindungi masyarakat di era digital.

D. Tantangan dalam Penegakan Hukum Siber

Perkembangan teknologi di era digital telah membawa banyak manfaat bagi kehidupan modern, namun juga diiringi dengan tantangan baru, salah satunya adalah meningkatnya ancaman kejahatan siber. Di Indonesia, kejahatan siber seperti peretasan, pencurian identitas, dan penipuan online menjadi isu yang semakin mendesak untuk diatasi. Dampak dari kejahatan ini sangat luas, mulai dari kerugian finansial hingga ancaman terhadap privasi dan keamanan nasional. Pemerintah dan aparat hukum di Indonesia berusaha untuk merespons situasi ini melalui berbagai kebijakan dan regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)[19].

Namun, tantangan yang dihadapi dalam implementasinya masih sangat signifikan. Upaya penegakan hukum terhadap kejahatan siber di Indonesia menemui berbagai kendala yang berakar pada keterbatasan teknis, kurangnya kerjasama internasional, serta rendahnya kesadaran masyarakat terhadap pentingnya keamanan digital. Tantangan ini menunjukkan bahwa untuk mencapai sistem keamanan siber yang efektif, diperlukan pendekatan yang lebih komprehensif dan kolaboratif. Berikut ini akan diuraikan secara lebih mendalam mengenai tantangan-tantangan utama dalam penegakan hukum siber di Indonesia.

Berikut adalah beberapa tantangan utama yang dihadapi dalam penegakan hukum siber di Indonesia:

1. Kesenjangan Teknis

Penegakan hukum siber di Indonesia mengalami tantangan besar dalam hal kesenjangan teknis, terutama dalam hal teknologi dan sumber daya manusia yang berkompeten. Teknologi yang dibutuhkan untuk mengidentifikasi, melacak, dan menangani kejahatan siber terus berkembang pesat, sementara penegak hukum di Indonesia sering kali tidak memiliki akses ke perangkat dan pelatihan yang sesuai. Dalam beberapa kasus, kendala ini menghambat kemampuan pihak berwenang untuk menyelidiki kejahatan yang

[19]Wildan Fahriza And Muhammad Arif Sahlepi, 'Effectiveness Of Law Enforcement Against Cybercrime In Indonesia On Hacking Crimes And The Role Of The Ite Law', Law Synergy Conference (Lsc) 1, No. 1 (2024): 179–85, Https://Conference.Sinergilp.Com/Index.Php/Lsc/Article/Download/25/30/103.

kompleks dan canggih, seperti ransomware atau serangan *Advanced Persistent Threat* (APT), yang membutuhkan pengetahuan mendalam dan alat forensik digital mutakhir.[20]

Selain itu, banyak aparat hukum yang belum mendapatkan pelatihan khusus mengenai keamanan siber, yang sangat diperlukan dalam era digital saat ini. Peningkatan kapasitas teknis dan investasi dalam teknologi forensik digital merupakan kunci untuk mengurangi kesenjangan ini. Negara-negara maju telah memperkenalkan pelatihan berkelanjutan untuk aparat penegak hukum guna memperbarui pengetahuan mereka tentang ancaman baru dan teknologi penanganannya.[21]

2. Kerjasama Internasional yang Terbatas

Karakteristik kejahatan siber yang lintas batas menambah kompleksitas dalam penanganannya. Pelaku kejahatan siber sering kali beroperasi dari luar negeri atau menggunakan server di negara lain, sehingga penegakan hukum di satu negara saja, seperti Indonesia, tidak cukup untuk menuntut mereka. Kejahatan siber seperti ini memerlukan kerjasama antarnegara dan koordinasi melalui organisasi internasional. Di Indonesia, masih ada keterbatasan dalam hal kerjasama dengan negara-negara lain atau organisasi internasional terkait penegakan hukum siber, yang menghambat proses investigasi lintas batas.[22]

Indonesia telah menjalin kerjasama melalui forum-forum internasional seperti INTERPOL, namun belum pada tingkat yang optimal untuk memudahkan ekstradisi atau penuntutan lintas negara. Negara-negara seperti Amerika Serikat dan Uni Eropa telah membentuk kerangka kerja bersama seperti *Budapest Convention on Cybercrime* untuk memfasilitasi pertukaran informasi dan bantuan hukum dalam kejahatan siber lintas batas. Perjanjian seperti ini dapat menjadi contoh bagi Indonesia untuk meningkatkan efektivitas dalam menangani kasus siber yang melibatkan pelaku internasional.

3. Kurangnya Kesadaran Publik

---

[20]'Indonesia's Cybersecurity: 94% Of Organizations Faced A Breach In The Past Year', Insightech Asia, 17 April 2023, Https://Insightechasia.Com/Cyber-Security/Indonesias-Cybersecurity-94-Of-Organizations-Faced-A-Breach-In-The-Past-Year/#Google_Vignette; 'Countering The Cyber Enforcement Gap: Strengthening Global Capacity On Cybercrime', 27 May 2020, Https://Www.Thirdway.Org/Report/Countering-The-Cyber-Enforcement-Gap-Strengthening-Global-Capacity-On-Cybercrime; Katya Loviana, 'Cybersecurity And Cyber Resilience In Indonesia: Challenges And Opportunities' (Yogyakarta, 10 May 2022), Https://Digitalsociety.Id/Id/.

[21]'Indonesia's Cybersecurity: 94% Of Organizations Faced A Breach In The Past Year'.

[22]Loso Judijanto, Melyana R Pugu, And Yuarini Wahyu Pertiwi, 'Indonesian Criminal Law Reform In The Face Of Cybercrime', International Journal Of Society Reviews (Injoser) 2, No. 6 (2024): 1548–61.

Tantangan lainnya adalah rendahnya tingkat kesadaran masyarakat tentang pentingnya keamanan siber dan perlindungan data pribadi. Banyak pengguna internet di Indonesia yang belum memahami risiko kejahatan siber dan cara melindungi diri mereka. Misalnya, sering kali individu maupun perusahaan mengabaikan protokol keamanan dasar, seperti pembaruan perangkat lunak atau penggunaan kata sandi yang kuat. Hal ini membuat mereka rentan terhadap ancaman siber seperti *phishing*, *malware*, atau bahkan *ransomware*.[23]

Rendahnya kesadaran publik ini juga diperburuk oleh kurangnya kampanye edukasi yang masif dan berkelanjutan dari pemerintah serta sektor swasta. Program pendidikan dan pelatihan keamanan siber perlu diperkenalkan di kalangan masyarakat umum, khususnya bagi pengguna internet pemula, untuk menurunkan risiko kejahatan siber. Banyak negara telah sukses meningkatkan kesadaran keamanan digital melalui kampanye nasional, seperti program "*Cyber Smart Week*" di Australia, yang bisa dijadikan contoh bagi Indonesia .

E. Studi Kasus: Penanganan Kejahatan Siber di Berbagai Negara

Dalam penanganan kejahatan siber, beberapa negara maju telah mengembangkan regulasi dan sistem keamanan yang lebih terstruktur dibandingkan Indonesia. Berikut ini adalah beberapa contoh kebijakan siber yang diterapkan di Amerika Serikat dan Uni Eropa, serta pembelajaran yang dapat diambil untuk memperkuat sistem keamanan siber di Indonesia.

1. Amerika Serikat: *Cybersecurity Information Sharing Act* (CISA)

Amerika Serikat telah mengadopsi *Cybersecurity Information Sharing Act (CISA)*, sebuah undang-undang yang memungkinkan pemerintah dan sektor swasta untuk berbagi informasi terkait ancaman siber. UU ini mendorong perusahaan dan instansi pemerintah untuk berbagi intelijen siber secara aktif, yang memungkinkan pihak terkait mengidentifikasi dan menangkal ancaman siber secara lebih efektif. Dengan adanya berbagi informasi, perusahaan dapat belajar dari pengalaman insiden siber yang terjadi di organisasi lain, meningkatkan ketanggapan dalam menghadapi ancaman yang mungkin terjadi.

[23]Audria Putri And M. Irfan Yusuf, 'General Overview Of The Cyber Security In Indonesia's Digital Landscape Under Presidential Regulation No. 47 Of 2023 On National Cybersecurity Strategy And Cyber Crisis Management', Nusantara Legal Partnership, 8 February 2024, Https://Www.Mondaq.Com/Security/1421514/General-Overview-Of-The-Cyber-Security-In-Indonesias-Digital-Landscape-Under-Presidential-Regulation-No-47-Of-2023-On-National-Cybersecurity-Strategy-And-Cyber-Crisis-Management.

Selain itu, Amerika Serikat juga memiliki *Cybersecurity and Infrastructure Security Agency* (CISA), yang berperan sebagai pusat respons dan mitigasi ancaman siber pada tingkat nasional. Agen ini bertanggung jawab untuk merespons insiden keamanan siber secara cepat dan mengoordinasikan langkah mitigasi antara lembaga pemerintah dan sektor swasta. Mereka juga melakukan pemantauan rutin terhadap ancaman siber dan memberikan peringatan dini kepada organisasi yang berpotensi terkena serangan.[24]

Dengan model ini, penanganan kejahatan siber di Amerika Serikat menjadi lebih tanggap dan proaktif. Langkah ini juga diiringi dengan pelatihan khusus dan standar teknis yang harus diikuti oleh perusahaan-perusahaan besar yang bergerak dalam sektor kritis. Pelaksanaan CISA di Amerika Serikat menunjukkan bahwa kolaborasi erat antara pemerintah dan swasta, serta pembagian informasi secara terbuka, dapat meningkatkan efektivitas dalam menanggulangi serangan siber dan melindungi infrastruktur nasional yang penting.

Indonesia dapat memanfaatkan model kerja sama CISA dengan membangun platform berbagi informasi ancaman yang melibatkan sektor pemerintah, perusahaan teknologi, dan penyedia layanan internet lokal, untuk meningkatkan respons terhadap serangan lintas batas. Koordinasi ini dapat dipimpin oleh Badan Siber dan Sandi Negara (BSSN) sebagai lembaga pusat, dengan dukungan regulasi untuk memastikan kerahasiaan data yang dibagikan. Hingga tahun 2022, BSSN mencatat lebih dari 800 juta anomali siber di Indonesia, sebagian besar berupa malware dan serangan ransomware, yang menunjukkan urgensi koordinasi antarinstansi dan sinergi lintas sektor dalam penanganan ancaman siber.

2. Uni Eropa: *General Data Protection Regulation* (GDPR)

Uni Eropa menerapkan *General Data Protection Regulation* (GDPR), sebuah regulasi yang dirancang untuk melindungi data pribadi warga negara Uni Eropa. GDPR mewajibkan perusahaan untuk mengambil langkah-langkah yang jelas dalam melindungi data pengguna dan memberikan kontrol lebih besar bagi individu terhadap data pribadi mereka. Regulasi ini memberikan sanksi yang sangat tegas bagi perusahaan yang gagal melindungi data pribadi, termasuk denda yang bisa mencapai hingga 4% dari total

[24]Sean Atkins And Chappell Lawson, 'Cooperation Amidst Competition: Cybersecurity Partnership In The Us Financial Services Sector', Journal Of Cybersecurity 7, No. 1 (2 December 2021), Https://Doi.Org/10.1093/Cybsec/Tyab024.

pendapatan tahunan perusahaan atau 20 juta Euro, tergantung mana yang lebih besar.[25]

Salah satu aspek penting dalam GDPR adalah prinsip transparansi, di mana perusahaan harus memberi tahu pengguna tentang bagaimana data mereka akan digunakan, serta menyediakan opsi bagi pengguna untuk mengelola dan menghapus data mereka. Selain itu, GDPR mengharuskan perusahaan untuk melaporkan pelanggaran data pribadi dalam waktu maksimal 72 jam setelah kejadian, yang mendorong transparansi dan akuntabilitas yang tinggi dalam pengelolaan data.

GDPR juga menetapkan kewajiban untuk mempekerjakan petugas perlindungan data (*Data Protection Officer atau DPO*) bagi perusahaan besar dan organisasi publik. Petugas ini bertanggung jawab untuk memastikan kepatuhan organisasi terhadap regulasi perlindungan data dan melakukan audit keamanan data secara berkala. Implementasi GDPR di Uni Eropa menunjukkan pentingnya perlindungan data pribadi sebagai bagian integral dari keamanan siber secara keseluruhan.

Pendekatan yang diterapkan oleh Amerika Serikat melalui *Cybersecurity Information Sharing Act* (CISA) memperlihatkan bagaimana kolaborasi erat antara pemerintah dan sektor swasta mampu mempercepat respons dalam menghadapi ancaman siber yang kian kompleks. Model ini memungkinkan perusahaan dan instansi pemerintah untuk berbagi informasi intelijen siber secara aktif, sehingga masing-masing pihak dapat belajar dari insiden yang terjadi di organisasi lain dan mengembangkan langkah-langkah mitigasi yang lebih baik. Indonesia dapat mengadopsi mekanisme serupa dengan membangun jaringan pertukaran informasi yang melibatkan Badan Siber dan Sandi Negara (BSSN) serta perusahaan-perusahaan sektor kritis, guna memperkuat sinergi antarlembaga dalam menghadapi serangan siber yang bersifat lintas batas. Kolaborasi ini akan lebih efektif jika didukung oleh teknologi forensik digital dan pelatihan khusus yang dapat membantu aparat penegak hukum dalam menangani kasus-kasus kejahatan siber yang rumit.

Sementara itu, *General Data Protection Regulation* (GDPR) di Uni Eropa menunjukkan pentingnya perlindungan data pribadi sebagai bagian integral dari keamanan siber. Dengan mengharuskan perusahaan untuk menerapkan standar perlindungan data yang ketat dan memberikan sanksi yang besar bagi pelanggar,

[25]Stephen P. Mulligan, 'Crs Legal Sidebar Prepared For Members And Committees Of Congress Google Fined For Violation Of Eu Data Protection Law', 22 February 2019, Https://Crsreports.Congress.Gov ; Josephine Wolff And Nicole Atallah, 'Early Gdpr Penalties: Analysis Of Implementation And Fines Through May 2020', Journal Of Information Policy 11 (1 December 2021): 63–103, Https://Doi.Org/10.5325/Jinfopoli.11.2021.0063.

GDPR mendorong perusahaan untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan data. Indonesia dapat memperkuat Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan mewajibkan adanya petugas perlindungan data di perusahaan besar dan memperketat pelaporan pelanggaran data. Langkah ini bertujuan untuk memberikan kontrol lebih besar kepada individu atas data pribadi mereka serta memastikan bahwa perusahaan memiliki tanggung jawab yang lebih besar dalam menjaga keamanan data pengguna. Selain mengadopsi prinsip GDPR, Indonesia juga dapat memperkuat partisipasinya dalam kerja sama keamanan siber regional melalui ASEAN untuk mendorong harmonisasi regulasi di kawasan Asia Tenggara. Kerangka kerja seperti ASEAN Cybersecurity Cooperation dapat menjadi platform penting untuk menangani kejahatan siber lintas negara

Selain itu, baik Amerika Serikat maupun Uni Eropa menunjukkan bahwa peningkatan kesadaran publik mengenai pentingnya keamanan siber merupakan bagian penting dalam upaya mitigasi. Peningkatan literasi digital di Indonesia, yang pada 2022 memiliki skor indeks 3,54 (kategori sedang), menjadi prioritas untuk mengurangi risiko kejahatan siber. Kampanye literasi digital dapat melibatkan kementerian, platform media sosial, dan institusi pendidikan untuk membangun kesadaran publik tentang pentingnya keamanan data pribadi. Di Indonesia, pemerintah dapat menjalankan program nasional yang melibatkan berbagai pemangku kepentingan, termasuk kementerian, lembaga, dan organisasi non-pemerintah, untuk meningkatkan literasi digital dan kesadaran akan keamanan siber.

Implementasi dari pendekatan kolaboratif, regulasi yang ketat, serta edukasi publik yang berkelanjutan dapat memberikan landasan yang lebih kuat bagi Indonesia dalam menghadapi tantangan siber. Melalui adopsi prinsip-prinsip dari CISA dan GDPR, Indonesia dapat membangun ekosistem keamanan siber yang lebih tangguh, dengan kolaborasi antarinstansi dan sektor swasta yang terintegrasi dan pemahaman publik yang lebih mendalam akan pentingnya keamanan data. Langkah awal yang dapat diambil adalah menetapkan regulasi yang mewajibkan perusahaan di sektor kritis memiliki Data Protection Officer dan menerapkan standar pelaporan pelanggaran data dalam waktu 72 jam, seperti dalam GDPR. Standar ini dapat dimulai dari sektor keuangan, telekomunikasi, dan layanan publik yang menjadi target utama serangan siber

Penutup

Penelitian ini menunjukkan betapa pentingnya penguatan kebijakan kriminal untuk menangani kejahatan siber di Indonesia, terutama di tengah perubahan konstan teknologi digital. Pendekatan komprehensif diperlukan untuk mengatasi masalah yang dihadapi, seperti peretasan dan pencurian identitas. Ini

mencakup kerangka hukum yang adaptif, kerja sama antarinstansi yang strategis, dan peningkatan kesadaran masyarakat untuk memperjelas makna akan pentingnya keamanan digital. Kajian dan analisis yang dilakukan menunjukkan bahwa ada perbedaan antara peraturan saat ini dan bagaimana mereka diterapkan di lapangan, yang dapat menghambat upaya yang efektif untuk memerangi ancaman siber. Oleh karena itu, pemerintah Indonesia diharapkan dapat mempertimbangkan secara strategis untuk membuat kebijakan yang fleksibel dan memanfaatkan praktik terbaik dari negara lain untuk meningkatkan sistem keamanan sibernya.

Saran

1. **Penguatan Regulasi dan Implementasi UU ITE dan UU PDP**
   Pemerintah memiliki tanggung jawab untuk memastikan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) diterapkan dengan benar dan konsisten. Selain itu, regulasi harus secara teratur disesuaikan agar sesuai dengan kemajuan teknologi terbaru.
2. **Edukasi dan Literasi Digital bagi Masyarakat**
   Penting untuk meningkatkan kesadaran digital masyarakat dan literasi tentang keamanan siber. Pemerintah dapat bekerja sama dengan sektor swasta dan institusi pendidikan untuk melakukan kampanye dan program pelatihan yang berkelanjutan untuk meningkatkan pemahaman masyarakat tentang cara melindungi data pribadi mereka..
3. **Peningkatan Kapasitas dan Kompetensi Aparat Penegak Hukum**
   Penegak hukum harus mendapatkan pelatihan khusus terkait kejahatan siber agar mereka dapat menangani kasus yang lebih kompleks. Peningkatan kemampuan ini juga mencakup pemanfaatan teknologi forensik digital, yang dapat mempercepat proses penyidikan.
4. **Kerjasama Internasional dalam Penanganan Kejahatan Siber Lintas Batas**
   Karena kejahatan siber tersebar di seluruh dunia, Indonesia harus bekerja sama dengan negara lain dan organisasi internasional seperti INTERPOL untuk memudahkan investigasi dan ekstradisi pelaku kejahatan siber di seluruh dunia.
5. **Pembentukan Jaringan Pertukaran Informasi Siber**
   Pemerintah dapat membangun jaringan pertukaran informasi siber yang melibatkan Badan Siber dan Sandi Negara (BSSN) serta perusahaan-perusahaan sektor kritis. Hal ini bertujuan untuk mempercepat respons dalam menghadapi ancaman siber dan meningkatkan kemampuan antisipasi terhadap serangan yang mungkin terjadi.

Daftar Pustaka

Agustini, Pratiwi. 'Indeks Literasi Digital Indonesia Kembali Meningkat Tahun 2022'. *Kominfo*, 2023. https://aptika.kominfo.go.id/2023/02/indeks-literasi-digital-indonesia-kembali-meningkat-tahun-2022/.

Atkins, Sean, and Chappell Lawson. 'Cooperation amidst Competition: Cybersecurity Partnership in the US Financial Services Sector'. Journal of Cybersecurity 7, no. 1 (2 December 2021). https://doi.org/10.1093/cybsec/tyab024.

Cahyadi, Benny, Erdy Gian Gara, Putra Pratama, Ginanjar Fitriadi, Dwi Satya Arian, and Kepolisian Republik Indonesia Sespim Lemdiklat Polri Jl Raya Maribaya No. 'HACKER ANAK DALAM PERSPEKTIF TEORI DIFFERENTIAL ASSOCIATION: STUDI KASUS PERETASAN SITUS PENGADILAN NEGERI KABUPATEN KONAWE'. IKRAITH-HUMANIORA 8, no. 1 (March 2024): 329–40. https://doi.org/https://doi.org/10.37817/ikraith-humaniora.v8i1.

Chaterine, Rahel Narda, and Dani Prabowo. 'Bareskrim Tangkap Buron Kasus Penipuan Ratusan WNI Modus Lowongan Kerja'. Kompas.Com, July 2024. https://nasional.kompas.com/read/2024/07/19/16055431/bareskrim-tangkap-buron-kasus-penipuan-ratusan-wni-modus-lowongan-kerja.

Coloroso, Barbara, and Santi Indra Astuti. Stop Bullying: Memutuskan Rantai Kekerasan Anak Dari Prasekolah Hingga SMU. Jakarta: Serambi Ilmu Semesta, 2007.

'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime', 27 May 2020. https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. 'Cyber Risk and Cybersecurity: A Systematic Review of Data Availability'. The Geneva Papers on Risk and Insurance - Issues and Practice 47, no. 3 (17 July 2022): 698–736. https://doi.org/10.1057/s41288-022-00266-6.

Dani Ihkam, Muhammad, and I Gusti Ngurah Parwata. 'TINDAK PIDANA CYBER BULLYING DALAM PERSPEKTIF HUKUM PIDANA DI INDONESIA'. Jurnal Kertha Wicara. Vol. 9, n.d.

Diba Tanzilla, Farah, Margaretha Hanita, and Bondan Widiawan. 'Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law'. International Journal of Progressive Sciences and Technologies (IJPSAT 40, no. 2 (2023): 164–70.

Fadil Imran, Mohammad. 'Preventing and Combating Cybercrime in Indonesia'. International Journal of Cyber Criminology 17, no. 1 (2023): 223–35. https://doi.org/DOI:10.5281/zenodo.4766614.

Fahriza, Wildan, and Muhammad Arif Sahlepi. 'Effectiveness of Law Enforcement against Cybercrime in Indonesia on Hacking Crimes and the Role of the ITE Law'. Law Synergy Conference (LSC) 1, no. 1 (2024): 179–85.

https://conference.sinergilp.com/index.php/lsc/article/download/25/30/103.
Horan, Cecelia, and Hossein Saiedian. 'Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions'. Journal of Cybersecurity and Privacy 1, no. 4 (1 December 2021): 580–96. https://doi.org/10.3390/jcp1040029.
Hull, Gavin, Henna John, and Budi Arief. 'Ransomware Deployment Methods and Analysis: Views from a Predictive Model and Human Responses'. Crime Science 8, no. 1 (12 December 2019): 2. https://doi.org/10.1186/s40163-019-0097-9.
Hüsch, P., and J. Sullivan. 'Global Approaches to Cyber Policy, Legislation and Regulation'. The Royal United Services Institute for Defence and Security Studies, 26 April 2023. https://www.rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation.
InsighTech Asia. 'Indonesia's Cybersecurity: 94% of Organizations Faced a Breach in the Past Year'. 17 April 2023. https://insightechasia.com/cyber-security/indonesias-cybersecurity-94-of-organizations-faced-a-breach-in-the-past-year/#google_vignette.
Judijanto, Loso, Melyana R Pugu, and Yuarini Wahyu Pertiwi. 'INDONESIAN CRIMINAL LAW REFORM IN THE FACE OF CYBERCRIME'. International Journal of Society Reviews (INJOSER) 2, no. 6 (2024): 1548–61.
Katya Loviana. 'Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities'. Yogyakarta, 10 May 2022. https://digitalsociety.id/id/.
Kristianti, Livia. 'BSSN Ungkap Serangan Keamanan Siber Di 2022 Turun Dibanding 2021'. Antaranews.com, 2023. https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021.
M. Wantu, Frence. Pengantar Ilmu Hukum. 1st ed. Gorontalo: UNG Press, 2015.
Nurahman, Dwi. 'KEBIJAKAN PENEGAKAN HUKUM CYBERCRIME DAN PEMBUKTIAN YURIDIS DALAM SISTEM HUKUM PIDANA NASIONAL'. KeadilaN Jurnal Fakultas Hukum Universitas Tulang Bawang 17, no. 2 (1 January 2019). https://doi.org/10.37090/keadilan.v17i2.270.
Purba, Yedija Otniel, and Agus Mauluddin. 'Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online'. JCIC: Jurnal CIC Lembaga Riset Dan Konsultan Sosial-ISSN 5, no. 2 (2023): 55–66. https://doi.org/10.51486/jbo.v5i2.113.
Putra, Budi Kristian Bivanda. 'KEBIJAKAN APLIKASI TINDAK PIDANA SIBER (CYBER CRIME) DI INDONESIA'. Pamulang Law Review 1, no. 1 (15 July 2019): 1. https://doi.org/10.32493/palrev.v1i1.2842.
Putri, Audria, and M. Irfan Yusuf. 'General Overview Of The Cyber Security In Indonesia's Digital Landscape Under Presidential Regulation No. 47 Of 2023 On National Cybersecurity Strategy And Cyber Crisis Management'. Nusantara Legal Partnership, 8 February 2024. https://www.mondaq.com/security/1421514/general-overview-of-the-

cyber-security-in-indonesias-digital-landscape-under-presidential-regulation-no-47-of-2023-on-national-cybersecurity-strategy-and-cyber-crisis-management.

Razzaq, Abdul, Matthew Aditya, Amelia Widya, Octa Kuncoro Putri, Desta Lesmana Musthofa, and Pujo Widodo. 'Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator)'. Global Political Studies Journal 6 (2022). https://doi.org/DOI10.34010/gpsjournal.v6i1.

Reuters. 'Cyber Attack Compromised Indonesia Data Centre, Ransom Sought'. Reuters.Com, 24 June 2024. https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24.

Setiawan, Radita, and Muhammad Okky Arista. 'Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana'. RECIDIVE: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan 2, no. 2 (2013): 139–46. https://doi.org/https://doi.org/10.20961/recidive.v2i2.32324.

Stephen P. Mulligan. 'CRS Legal Sidebar Prepared for Members and Committees of Congress Google Fined for Violation of EU Data Protection Law', 22 February 2019. https://crsreports.congress.gov.

Widianingrum, Afifah Rizqy. 'ANALISIS IMPLEMENTASI KEBIJAKAN HUKUM TERHADAP PENANGANAN KEJAHATAN SIBER DI ERA DIGITAL'. JOURNAL IURIS SCIENTIA 2, no. 2 (27 July 2024): 90–102. https://doi.org/10.62263/jis.v2i2.40.

Wolff, Josephine, and Nicole Atallah. 'Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020'. Journal of Information Policy 11 (1 December 2021): 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063.

Biografi Singkat Penulis

Muhammad Arafat, S.H., M.H., C.Me., CLA., CIRP. 26 tahun, adalah mahasiswa doktoral di bidang Hukum Islam di Universitas Islam Indonesia. Saat ini, saya berprofesi sebagai advokat dengan pengalaman kurang lebih satu tahun. Dalam peran saya sebagai advokat, saya tidak hanya menangani berbagai kasus hukum, tetapi juga aktif memberikan penyuluhan hukum kepada masyarakat. Kegiatan penyuluhan ini bertujuan untuk meningkatkan pemahaman masyarakat mengenai hak-hak hukum mereka dan bagaimana hukum Islam dapat diterapkan dalam konteks modern. Saya berkomitmen untuk terus mengembangkan wawasan dan keahliannya dalam hukum Islam agar dapat memberikan kontribusi yang bermanfaat bagi masyarakat luas, serta membantu menciptakan kesadaran hukum yang lebih baik di Indonesia.

Alexander Tito Enggar Wirasto, S.H. umur 28 tahun. Saat ini saya menjadi praktisi di bidang hukum, sebagai seorang Advokat saya aktif di organisasi Advokat yakni PERADI dan menjabat sebagai Wakil Ketua Divisi Inovasi dan Kreatif pada Young Lawyer`s Committee PERADI Kota Yogyakarta, di samping itu saya juga menjabat sebagai Sekretaris pada Lembaga Bantuan Hukum Harapan di wilayah D.I.Yogyakarta. Sebagai praktisi saya juga aktif dalam memberikan penyuluhan hukum bagi masyarakat yang kurang mampu, dengan harapan meningkatkan edukasi hukum bagi masyarakat awam yang rentan akan ketidakadilan terkhusus agar semakin banyak masyarakat yang peduli akan hukum yang berlaku. Saya percaya hukum adalah panglima kehidupan yang menerangi jalan masa depan menuju Indonesia raya.