Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Kebijakan Hukum Pidana dalam Penanganan Kejahatan Siber

INFO PENULIS

Maria Ferba Editya
Universitas Quality Berastagi
maria.juntakk@gmail.com
+6285362134568

Hanna Niken Julia Sihotang
Universitas Quality Berastagi
HannaNikenJuliaSihotang@gmail.com

Orlando Benedivh Passia Sianipar
Universitas Quality Berastagi
OrlandoBenedivhPassiaSianipar@gmail.com

Trio Alpan Tarigan
Universitas Quality Berastagi
TrioAlpanTarigan@gmail.com

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 3, Desember 2025
https://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Editya, M. F., Sihotang, H. N. J., Sianipar, O. B. P., & Tarigan, T. A., (2025). Kebijakan Hukum Pidana dalam Penanganan Kejahatan Siber. *Arus Jurnal Sosial dan Humaniora, 5*(3),4680-4685.

Abstrak

Kebijakan hukum pidana adalah kebijakan yang diambil oleh negara melalui lembaga-lembaga berwenang untuk menerapkan peraturan yang diinginkan, diharapkan mampu mencerminkan apa yang ada dalam masyarakat dan mewujudkan cita-cita yang ada. Upaya dan kebijakan dalam membuat peraturan hukum pidana yang efektif pada dasarnya tidak bisa dipisahkan dari tujuan untuk mengatasi kejahatan. Oleh karena itu, kebijakan atau politik hukum pidana juga dianggap sebagai bagian dari politik dalam bidang kriminal. Dari perspektif politik kriminal, politik hukum pidana sejalan dengan definisi "kebijakan dalam mengatasi kejahatan melalui hukum pidana". Dunia saat ini dicirikan oleh kemajuan dalam teknologi informasi dan komunikasi yang mempengaruhi berbagai aspek kehidupan manusia. Adanya internet, sejenis media baru, dan kemajuan dalam teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan sosial, ekonomi, dan budaya dunia. Di era modern, kehidupan manusia sangat bergantung pada teknologi.Di satu sisi, adanya e-mail, e-commerce, cyber bank, bisnis online, internet banking, dan sebagainya adalah beberapa contoh bagaimana teknologi dapat memberikan banyak manfaat. Di sisi lain, juga berdampak negatif dengan munculnya kejahatan internet. Kemajuan teknologi informasi dan komunikasi dalam masyarakat saat ini tidak hanya membawa manfaat, tetapi juga menyebabkan ketidaksesuaian dalam penggunaannya, yang mengarah pada kejahatan siber. Dalam hal kaitannya dengan kebijakan hukum pidana, salah satu bagian dari dimensi kehidupan sosial saat ini yang perlu kebijakan hukum pidana yakni dampak teknologi informasi yang sangat berkembang dengan pesat menyebabkan banyak perubahan pada segi kehidupan sosial masyarakat, baik ekonomi, sosial politik. Sistem komunikasi dan interaksi, pendidikan, termasuk juga hukum. Teknologi informasI, internet pada awalnya dikembangkan semata-mata untuk memudahkan manusia dalam menjalankan rutinitas kehidupannya. Teknologi informasi di yakini membawa keuntungan yang besar bagi negara-negara di dunia. Artikel ini membahas urgensi tantangan penegakan hukum dalam kejahatan siber. Metode yang digunakan adalah penelitian hukum normative dengan pendekatan perundang-undangan dengan konseptual. Hasil penelitian

menunjukkan bahwa implementasi UU ITE masih menghadapi berbagai kendala, seperti cakupan hukum yang terbatas, lemahnya kapasitas penegakan hukum, rendahnya kesadaran masyarakat akan keamanan digital, serta karakteristik kejahatan siber yang lintas batas negara. Selain itu, meningkatnya ancaman terhadap infrastruktur vital dan data sensitif negara menunjukkan perlunya penguatan kerangka hukum yang lebih adaptif dan komprehensif.

Kata Kunci: Kebijakan, Hukum Pidana, Kejahatan Siber

Abstract

Criminal law policy is a policy adopted by the state through authorized institutions to implement desired regulations, expected to reflect what exists in society and realize existing ideals. Efforts and policies in creating effective criminal law regulations are essentially inseparable from the goal of overcoming crime. Therefore, criminal law policy or politics is also considered part of politics in the criminal field. From a criminal politics perspective, criminal law politics is in line with the definition of "policy in overcoming crime through criminal law." The world today is characterized by advances in information and communication technology that affect various aspects of human life. The existence of the internet, a type of new media, and advances in information and communication technology have brought major changes in the social, economic, and cultural life of the world. In the modern era, human life is highly dependent on technology. On the one hand, the existence of e-mail, e-commerce, cyber banking, online business, internet banking, and so on are some examples of how technology can provide many benefits. On the other hand, it also has a negative impact with the emergence of internet crime. The advancement of information and communication technology in today's society not only brings benefits but also leads to inappropriate use, leading to cybercrime. In relation to criminal law policy, one aspect of current social life that requires criminal law policy is the impact of rapidly developing information technology, which has led to numerous changes in social life, both economic and socio-political. These include communication and interaction systems, education, and even law. Information technology, including the internet, was initially developed solely to facilitate human daily routines. Information technology is believed to bring significant benefits to countries worldwide. This article examines the urgent challenges of law enforcement in cybercrime. The method used is normative legal research with a conceptual legislative approach. The results show that the implementation of the ITE Law still faces various obstacles, such as limited legal coverage, weak law enforcement capacity, low public awareness of digital security, and the cross-border nature of cybercrime. Furthermore, the increasing threats to vital infrastructure and sensitive state data demonstrate the need to strengthen a more adaptive and comprehensive legal framework.

Key Words: Policy, Criminal Law, Cybercrime

A. Pendahuluan

Dinamika IPTEK dalam kehidupan masyarakat saat ini selain memberikam dampak positif, tetapi juga memberikan dampak negatif dari ketidaksesuaian penggunaannya. (Audrey. 2016) Dalam perspektif hukum pidana, upaya penanggulangan cyber crime dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek pembuktian dan alat bukti), dan aspek yurisdiksi.(Barda Nawawi Arief. 2005) Berkaitan dengan hal tersebut, perumusan tindak pidana di dalam KUHP masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan cyber crime. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan hitech crime (kejahatan berteknologi tinggi) yang sangat bervariasi. Misalnya, untuk menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik, dalam KUHP tidak ada ketentuan khusus mengenai pembuatan kartu kredit, yang ada hanya ketentuan mengenai; sumpah/keterangan palsu tercantum pada Bab IX Pasal 242 KUHP, pemalsuan mata uang dan uang kertas pada Bab X Pasal 244-252 KUHP, tentang pemalsuan pada Bab XI Pasal 253-262 KUHP, pemalsuan surat pada Bab XII Pasal 263-276 KUHP.

Aspek pokok aktivitasnya, cyber crime dilakukan lebih menitikberatkan pada penyerangan content, computer system dan communication system milik orang lain, baik secara personal maupun umum di dalam cyber space. Untuk itu, diperlukan pengamanan sebuah sistem untuk

mencegah terjadinya perusakan. Penanggulangan cyber crime dilakukan dengan pencegahan dan penegakan hukum, demi tercapainya supremasi hukum. Apabila dibiarkan terus menerus, dapat mengganggu keamanan baik secara nasional maupun internasional. Sesungguhnya cyber crime sudah mengganggu keamanan dalam negeri maupun luar negeri, sehingga diperlukan langkah-langkah strategis aparat penegak hukum untuk menanggulanginya

Lahirnya Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) telah dinilai mampu mengakomodir jenis kejahatan yang merupakan pengembangan terhadap kejahatan melalui media internet. Selain itu, undang-undang tersebut diharapkan menjadi jawaban konkrit terhadap masalah yang dihadapi oleh aparatur penegak hukum.

Meningkatnya cyber crime seperti misalnya kejahatan carding (penipuan kartu kredit), skimming ATM/EDC, hacking, cracking, phishing, malware (virus/worm/trojan/bot), cybersquatting, pornografi ,perjudian online, kejahatan transnasional (perdagangan narkoba, mafia, terorisme, pencucian uang,perdagangan manusia, ekonomi bawah tanah) perlu dilakukan perlindungan data secara umum dalam hal iniperlunya aturan hukum yang mengikat yang selanjutnya ditegakkan untuk melindungi informasi pribadi danmemastikan bahwa subjek data tetap mengendalikan informasi mereka (Haingo Rabarijaona dan Devina Arifani,2020). Peraturan tersebut memerlukankepastian pengelolaan data dan informasi, khususnya dalam pengelolaan data pribadi, karena tanpapengelolaan data yang baik dan benar maka akan menimbulkan penyalahgunaan dan serangan cybercrime.Oleh karena itu, diperlukan analisis manajemen risiko dalam menghadapi serangan cybercrime.(Angga Dewanto Basari, Muhammad Syauqillah, dan Asep Usman Ismail, 2020) Karena serangan cybercrime ini berpotensi kehilangan informasi data, permasalahan seperti ini masih sulit untukdiatasi. Kejahatan mengenai data pribadi sering kali ditemukan dalam suatu perusahaan karena dalam hal inimereka perlu mempelajari bagaimana data tersebut dikelola dan diamankan dengan baik dan benar. Kriminalisasi cybercrime di Indonesia, khususnya dalam UU ITE, dapat dibagi menjadi dua kategori,yaitu tindakan yang menggunakan komputer sebagai sarana kejahatan dan tindakan yang menjadikankomputer sebagai target kejahatan. Kejahatan yang menggunakan komputer sebagai sarana segala perbuatanyang memanfaatkan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukankejahatan di dunia maya, bukan di dunia nyata.

B. Metodologi

Penulis menggunakan metode yuridis normatif, yang melibatkan analisis terhadap peraturan perundang-undangan, literatur hukum, dan dokumen terkait lainnya yang relevan dengan kebijakan hukum pidana dalam penanggulangan kejahatan siber di Indonesia. Metode ini dipilih karena memungkinkan analisis mendalam terhadap aspek hukum yang berlaku.

1. *Research Design*
   Pendekatan yang digunakan adalah pendekatan konseptual (conceptual approach) yang mana digunakan untuk mengkaji konsep-konsep hukum yang terkait.
2. *Technique of Data Collection*
   Data dalam penelitian ini dikumpulkan melalui studi pustaka meliputi analisis terhadap peraturan perundangundangan, putusan pengadilan, jurnal hukum, buku teks, dan dokumen terkait lainnya.
3. *Technique of Data Analysis*
   Analisis dilakukan dengan menggunakan pendekatan deskriptif analitis, yaitu menggambarkan kebijakan hukum pidana yang ada dan menganalisis efektivitasnya dalam penanggulangan cybercrime

C. Hasil dan Pembahasan

1. Hasil

Kebijakan hukum terhadap kejahatan siber di Indonesia berfokus pada Undang-Undang ITE (UU No. 11 Tahun 2008 bersamaan dengan Undang-Undang No. 19 Tahun 2016 serta Undang-Undang No. 1 Tahun 2024) yang mengatur mengenai transaksi digital dan elektronik, serta Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) yang bertujuan mengamankan data pribadi, disertai dengan Kitab Undang-Undang Hukum Pidana Baru (UU No. 1 Tahun 2023). Upaya untuk mengatasi kejahatan siber ini meliputi penerapan sanksi pidana terhadap peretasan, pencurian informasi, penipuan melalui internet, serta penyebaran konten yang dilarang. Akan tetapi, terdapat beberapa kendala dalam pelaksanaannya, seperti adanya

interpretasi yang berbeda terhadap beberapa pasal, kesulitan dalam mengumpulkan bukti digital, dan kurangnya koordinasi antar lembaga. Oleh karena itu, sangatlah penting untuk meningkatkan kapasitas sumber daya manusia dan melakukan revisi terhadap regulasi yang lebih responsif.

Kebijakan untuk melindungi data memerlukan analisis yang sangat mendalam. Saat ini, teknologi informasi memiliki peranan penting dan memberikan pengaruh besar terhadap segala aspek kehidupan manusia. Aturan mengenai teknologi informasi yang ingin diterima oleh publik harus memperhatikan berbagai harapan dan berbagai kepentingan, yang perlu disesuaikan dan diharmonisasikan, serta kebijakan yang berkaitan dengan kejahatan yang memanfaatkan teknologi harus berhubungan dengan hukum pidana, termasuk dalam bidang kebijakan pidana. (Arief, 2005)

Kebijakan pencegahan cybercrime dengan hukum pidana mencakup bidang kebijakan penal yangmerupakan bagian dari kebijakan kriminal. Dari sudut pandang kebijakan pidana, upaya pencegahankejahatan (termasuk penanggulangan cybercrime) tidak dapat dilakukan hanya secara parsial dengan hukumpidana (hukum pidana) namun hal tersebut juga harus dilakukan dengan pendekatan sistematik. (James,2020).

Penggunaan hukum pidana selama ini dianggap sebagai hal yang normal, artinya dengan kondisi tersebut eksistensinya sudah tak lagi dipermasalahkan Dalam Kitab Undang-Undang Hukum Pidana Kitab Undang–Undang Hukum Pidana yang biasa disingkat menjadi KUHP merupakan sistem utama bagi peraturan-peraturan hukum pidana di Indonesia. Perumusan tindak pidana yang tercantum dalam KUHP mayoritas masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan dari cyber crime itu sendiri. Beberapa peraturan perundang- undangan yang berhubungan dengan tindak pidana teknologi informasi diluar dari pengaturan KUHP yaitu:

1. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi
2. Undang-Undang Nomor 19 Tahun 2002 TentangHak Cipta
3. Undang-Undang Nomor 25 Tahun 2003 Tentang Perubahan atas Undang- Undang
4. Nomor 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang
5. Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Kebijakan hukum pidana dalam penanggulangan kejahatan menggunakan teknologi bukanlah sekedar pembuatan kebijakan tetapi memperhatikan harmonisasi kebijakan penal di berbagai negara, melakukan kriminalisasi kejahatan menggunakan teknologi dan informasi ada beberapa hal yang harus diperhatikan oleh pembetuk undang-undang yaitu:

a. Kriminalisasi harus merupakan Upaya yang mendukung tujuan akhir kebijakan kriminal, yaitu melindungi dan mensejahterakan masyarakat.
b. Perbuatan yang akan dikriminalisasi tersebut benar-benar dicela oleh masyarakat.
c. Perlu diperhatikan tentang keuntungan dan kerugian kriminalisasi.
d. Perlu diperhitungkan agar tidak terjadi over-kriminalisasi yang dapat berpengaruh secra sekunder terhadap kepentingan masyarakat.
e. Perlu disesuaikan antara kemampuan penegak hukum dengan penegakan hukum.

Kebijakan hukum pidana adalah bagaimana hukum pidana dapat dirumuskansecara memadai, memberikan pedoman bagi pembentuk undang-undang, dan melaksanakan hukum pidana.Kebijakan legislatif sangat menentukan dalam tahap-tahap berikutnya karena pada saat akan dibuat peraturanperundang-undangan pidana sudah ditentukan tujuan yang ingin dicapai. Jika dilihat pada Pasal 26 ayat (2)UU ITE, hal semacam itu tidak memberikan sanksi pidana kepada pelakunya. Dalam kasus ini, korban hanyamenggugat secara perdata. Selain itu, Pasal 26 UU ITE hanya tentang perlindungan esensial. Pakar teknologiinformasi menilai Pasal 26 UU ITE memiliki kelemahan. Kekurangannya adalah tidak adanya perlindunganpengguna yang data pribadinya digunakan untuk memperoleh keuntungan tertentu bagi perusahaan.Keamanan data dimaksudkan untuk meningkatkan keamanan data dan berfungsi untuk 1) Melindungi dataagar tidak dapat dibaca oleh orang yang tidak berkepentingan; 2) Mencegah orang yang tidak berkepentinganmemasukkan atau menghapus data.

2. Pembahasan

Kejahatan siber semakin meningkat tidak hanya dalam hal frekuensi, tetapi juga dalam hal kompleksitasnya. Menurut Supriyadi (2022), kejahatan siber kini melibatkan jaringan internasional yang terorganisir, sehingga membutuhkan kerja sama lintas negara untuk dapat ditangani secara efektif. Selain itu, pelaku kejahatan siber seringkali memanfaatkan kecanggihan teknologi untuk menyembunyikan identitas mereka, yang membuat proses penegakan hukum

menjadi semakin sulit. Hal ini menunjukkan bahwa hukum pidana konvensional mungkin tidak cukup untuk menangani kejahatan siber yang bersifat lintas batas (Supriyadi,2022).

Meningkatnya cyber crime seperti misalnya kejahatan carding (penipuan kartu kredit), skimming ATM/EDC, hacking, cracking, phishing, malware (virus/worm/trojan/bot), cybersquatting, pornografi, perjudian online, kejahatan transnasional (perdagangan narkoba, mafia, terorisme, pencucian uang, perdagangan manusia, ekonomi bawah tanah) perlu dilakukan perlindungan data secara umum dalam hal ini perlunya aturan hukum yang mengikat yang selanjutnya ditegakkan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasi mereka. (Haingo dan Devina, 2020)

Tinjauan Umum Tentang Cyber Crime Istilah cyber crime saat ini merujuk pada suatu tindakan kejahatan yang berhubungan denga cyber space atau dunia maya dan tindakan kejahatan tersebut menggunakan komputer. Beberapa ahli yang menyakan antara tindak kejatan cyber dengan tindak kejahatan komputer, dan terdapat juga yang membedakan diantara keduanya. Dalam beberaoa literatur, cyber crime sering di identikkan sebagai computer crime. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mengartikan cyber crime sebagai kejahatan di bidang computer. secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Menurut freddy haris, cyber crime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

Kualifikasi kejahatan dunia maya (cyber crime) sebagaimana dalam buku Barda Nawawi Arief, adalah kualifikasi (cyber crime) menurut Convention on cybercrime 2001 di Budapest Hongaria, yaitu :

1) Illegal Interception Sengaja dan tanpa hak mendengar atau menangkap secara diam- diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.
2) Data Interference Sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer. System Interference Sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer. Misuse of Devive Penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code). Computer Related Forgery Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik) Computer Related Fraud Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan oranglain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Dalam menanggulangi cyber crime perlu dilakukan upaya komprehensif. Pencegahan dan penanggulangan kejahatan dilakukan dengan pendekatan integral antara kebijakan penal dengan kebijakan non penal. Kebijakan penal memiliki beberapa keterbatasan dan kelemahan yakni bersifar fragmatis,individualitik, lebih bersifat represif dan harus didukung dengan infratruktur yang memerlukan biaya tinggi (Hatta,2010) .Dengandemikian maka penanggulangan kejahatan lebihbaik dilakukan dengan menggunakan kebijakannonpenal yang bersifat preventif. Kebijakan dalampenanggulangan cybercrime dapat dilakukan denganduaacara yakni:

a. Kebijakan penal.
b. Kebijakan non penal.

Kebijakan penal adalah kebijakan yang terkait dengan penggunaan sanksi pidana dalam penyelesaian kasus kejahatan di dunia maya. Kebijakan penal dapat dilakukan melalui cara-cara berikut:

a. Kriminalisasi perbuatan dalam undang-undang sehingga perbuatan tersebut termasuk kejahatan di dunia maya.
b. Harmonisasi ketentuan hukum nasional dengan hukum internasional dalam memberantascy bercrime.
c. Penegakan hukum melalui penjatuhan sanksi pidana bagi pelaku cybercrime.

Politik hukum pidana dalam penanggulangan cybercrime melalui sarana penal perlu diimbangi denggan kebijakan non penal. Kebijakan non penal yang dapat dilakukan adalah sebagai berikut (Soejadi,2017) :

a. Menyusun kebijakan di luar hukum pidana yang mendukung upaya pencegahan cybercrime,seperti melalui kebijakan anti-kebencian, kebijakan anti-bullying dan kebijakan berinternet sehat melalui sistem pendidikan.

b. Melakukan sosialisasi terhadap potensi kejahatan di dunia maya dengan mengedukasi masyarakat pengguna internet untuk tidak mencantumkan identitas pribadi, bertransaksi ditempat dengan fasilitas internet yang aman dan sebagainya
c. Membangun kerjasama dengan pihak swasta untuk membangun sistem keamanan di dunia maya.
d. Membentuk jaringan kelembagaan dalam mencegah cybercrime baik dalam tataran nasional maupun dalam tingkat internasional.
e. Kerjasama internasional dalam penanggulangan cybercrime sangat diperlukan mengingat cybercrime merupakan kejahatan transnasional yang terorganisir.

D. Kesimpulan

Pertama dan terpenting, sistem penegakan hukum Indonesia dalam hal penanggulangan kejahatan cyber masih kurang efektif. Faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas penegakan hukum, dan faktor masyarakat adalah empat faktor yang dapat mempengaruhi penegakan hukum terhadap cyber crimes. Dari keempat faktor tersebut, faktor hukum (substansi hukum), yang banyak mengandung kelemahan dan faktor penegak hukum, adalah yang paling berpengaruh pada kelemahan penegakan hukum saat ini terhadap penanggulangan cyber crimes dalam anatomi kejahatan transnasional.

Kedua, kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia cyber yang semakin canggih. Hal ini disebabkan tindak pidana teknologi informasi yang tidak mengenal batas-batas teritorial dan beroperasi secara maya. Oleh karena itu, menuntut pemerintah harus selalu berupaya mengantisipasi aktivitas- aktivitas baru yang diatur oleh hukum yang berlaku.

Ketiga, walaupun di Indonesia sudah terdapat aturan hukum yang mengatur tentang tindak pidana teknologi informasi secara jelas, haruslah aturan tersebut diperbarui seiring dengan perkembangan zaman yang semakin maju dan semakin banyaknya juga jenis cyber crime yang berbeda bentuknya yang mungkin akan terjadi di masa yang akan datang.

Keempat, pentingnya masyarakat dapat memahami dan dapat membedakan antara virtual police dan cyber police sebagai aparat yang ikut menanggulangi cyber crime. Kesadaran masyarakat akan hukum juga merupakan salah aspek penting untuk melaraskan tujuan agar tercapainya pemberantasan cyber crime yang marak terjadi.

E. Referensi

Abdillah, A., Muhtarom, M., & Ismiyanto. (2022). Kebijakan Penanggulangan Kejahatan Tindak PidanaTeknologi Informasi. *Journal UNIBA, 34*(2).

Adhi, M. I., & Soponyono, E. (2021). Crime Combating Policy of Carding in Indonesia in the PoliticalPerspective of Criminal Law. *Law Reform, 17*(2).

Arief, B. N. (2005). *Pembaharuan hukum pidana dalam perspektif kajian perbandingan*. Citra Aditya Bakti.

Basari, A. D., Syauqillah, M., & Ismail, A. U. (2020). Kajian Penerapan Aturan Kegiatan Terorisme di Media Sosial*. Jurnal Studi Strategis dan Global, 3*(2*),* 5.

Haingo Rabarijaona dan Devina Arifani, (2020), Perlindungan Hukum Terhadap Pegawai/Pekerja Yang Mengalami Dampak Digitalisasi Hubungan Kerja. *Jurnal Pembaharuan Hukum, 7*(3)211.

Hartati, S., & Karyono, H. (2022). Implementation of The Law on Information and Electronic Transactionsand Pancasila Law Enforcement Related to Cybercrimes in Indonesia. *International Journal ofEducational Research & Social Sciences, 3*(1).

Hatta, M. (2010). *Kebijakan politik kriminal: Penegakan hukum dalam rangka penanggulangan kejahatan*. Pustaka Pelajar.

Popham, J., McCluskey, M., & Ouellet, M. (2020). Exploring Police-Reported Cybercrime In Canada Variation AndCorrelates. *Policing: An International Journal, 43*(1)35.

Soejadi, H. R. (2017). Refleksi mengenai hukum dan keadilan, aktualisasinya di Indonesia. *Jurnal Ketahanan Nasional*, *8*(2), 1-18.

Sudjito, B., Majid, A. S. F. & Ruslijanto, P. A. (2016). Tindak Pidana Pornografi dalam Era Siber di Indonesia*. Jurnal Wacana, 19*(2), 1.

Supriyadi, A. (2022). Dinamika kejahatan siber dan tantangan hukum lintas batas. *Jurnal Keamanan Siber, 14*(1), 15-29.