Indragiri Law Review
Pascasarjana Magister Ilmu Hukum Universitas Islam Indragiri
Vol. 2, No. 1, Juli 2023 ISSN: 3031-4186

Kebijakan Hukum Pidana untuk Penanggulangan *Cyber Crime* di Indonesia

Zainuddin Kasim
Magister Hukum, Universitas Islam Indragiri
acangadvokatkampoeng@gmail.com

Abstract

This research discusses the importance of criminal law policy in tackling cybercrime in Indonesia, focusing on the role of legal politics, existing criminal law policies, and eradication strategies. The method used is normative juridical analysis to explore relevant laws, legal literature, and relevant documents. The main findings include the complexity of regulations that are still inadequate to address the fast-growing dynamics of cybercrime. Indonesia still faces challenges in dealing with increasingly sophisticated and intense cybercrime. The conclusions of this study emphasize the need for more adaptive and comprehensive legal reforms to respond to the rapidly growing threat of cybercrime. Recommendations include strengthening international cooperation, increasing the capacity of law enforcement officers, and public education and awareness on digital security. With proper implementation, Indonesia is expected to increase the effectiveness of cybercrime countermeasures, protect digital assets, and minimize the negative impact on individuals, companies, and the country as a whole.

Kata Kunci:

Cybercrime
Kebijakan hukum
Politik Hukum

Abstrak

Penelitian ini membahas pentingnya kebijakan hukum pidana dalam penanggulangan *cybercrime* di Indonesia, dengan fokus pada peran politik hukum, kebijakan hukum pidana yang ada, dan strategi pemberantasan. Metode yang digunakan adalah analisis yuridis normatif untuk mengeksplorasi undang-undang terkait, literatur hukum, dan dokumen relevan. Temuan utama mencakup kompleksitas regulasi yang masih belum memadai untuk mengatasi dinamika *cybercrime* yang cepat berkembang. Indonesia masih menghadapi tantangan dalam menghadapi kejahatan siber yang semakin canggih dan intens. Kesimpulan dari penelitian ini menekankan perlunya pembaharuan hukum yang lebih adaptif dan komprehensif untuk menanggapi ancaman kejahatan siber yang berkembang pesat. Rekomendasi meliputi penguatan kerjasama internasional, peningkatan kapasitas aparat penegak hukum, serta pendidikan dan kesadaran masyarakat tentang keamanan digital. Dengan implementasi yang tepat, diharapkan Indonesia dapat meningkatkan efektivitas penanggulangan *cybercrime*, melindungi aset digital, dan meminimalisir dampak negatif terhadap individu, perusahaan, dan negara secara keseluruhan.

Corresponding Author:

Zainuddin Kasim
Magister Hukum
Universitas Islam Indragiri
acangadvokatkampoeng@gmail.com

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah memberikan berbagai manfaat signifikan dalam kehidupan manusia, namun di sisi lain juga membuka peluang bagi berbagai bentuk kejahatan baru, termasuk kejahatan siber (*cybercrime*). *Cybercrime* merupakan tindakan ilegal yang dilakukan melalui jaringan komputer atau internet, mencakup berbagai aktivitas seperti penipuan online, pencurian identitas, penyebaran malware, hingga serangan terhadap sistem informasi suatu negara. Kejahatan ini tidak hanya merugikan individu dan perusahaan, tetapi juga dapat mengancam keamanan nasional. Oleh karena itu, penanggulangan *cybercrime* telah menjadi isu krusial dalam kebijakan hukum pidana di berbagai negara, termasuk Indonesia.

Satu dekade terakhir perkembangan digital di Indonesia sangat meningkat seiring dengan migrasi bisnis dan konsumen ke dunia digital. Namun, perkembangan dan adopsi teknologi digital yang berkelanjutan, jika tidak dibentengi dengan praktik keamanan siber yang efektif, dapat menimbulkan potensi risiko dan kerentanan yang dapat dieksploitasi oleh penjahat siber. Risiko keamanan siber menjadi semakin sistematis dan parah di Indonesia, yang tidak hanya membahayakan institusi pemerintah dan bisnis tetapi juga individu. Pada tahun 2022, Indonesia mencatat hampir satu miliar anomali lalu lintas yang terkait dengan potensi serangan siber, sehingga diperlukan tindakan cepat untuk melindungi aset digital. Hingga saat ini, Indonesia sangat rentan terhadap pelanggaran data dan serangan phishing. Sebanyak kurang lebih 15 juta pelanggaran data online tercatat sepanjang tahun 2022, yang meningkatkan kekhawatiran terkait pelanggaran privasi data dan undang-undang perlindungan data di negara ini. Kurangnya tenaga profesional keamanan siber dan kurangnya kesadaran tentang ancaman siber berkontribusi pada ketidakmampuan Indonesia untuk memenuhi standar keamanan siber tertentu, membuat negara ini rentan terhadap serangan. Indonesia masih berjuang untuk mencegah dan mengelola ancaman siber dan insiden siber, dengan skor hanya 63,64 pada Indeks Keamanan Siber Nasional (NCSI). Hal ini juga tercermin dari pendapatan pasar keamanan siber Indonesia yang relatif rendah, yang saat ini berada di peringkat keenam di antara negara-negara Asia Pasifik[1].

Menurut World Bank, berdasarkan data ITU (International Telecommunication Union) porsi pengguna internet di dunia adalah sekitar 49 persen populasi pada tahun 2017, porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7 persen. Serupa dengan hal tersebut, Internet World Stats memperkirakan porsi pengguna internet di dunia adalah sebesar 64,2 persen populasi pada kuartal pertama tahun 2021. Adapun jumlah pengguna internet yang diperkirakan itu adalah sebanyak lebih dari 5 miliar, jumlah tersebut meningkat sekitar 1.300 persen dibandingkan tahun 2000.

Peningkatan jumlah pengguna internet di dunia tidak terlepas dari peningkatan jumlah ancaman ataupun serangan siber (cyber attack). Khusus Indonesia, BSSN (Badan Siber dan Sandi Negara) mencatat pada tahun 2018 ada 12,8 juta serangan. Pada tahun 2019 melonjak 98,2 juta serangan, selanjutnya pada tahun 2020 ada sebanyak 74,2 juta serangan. Total trafik anomali di Indonesia selama tahun 2023 adalah 403.990.813 anomali tentunya hal ini meningkat jauh dari tahun sebelumnya.[2]Selain itu, laporan dari Kaspersky pada tahun yang sama menunjukkan bahwa Indonesia menjadi salah satu negara dengan jumlah serangan siber tertinggi di dunia. Fakta-fakta ini menunjukkan bahwa *cyber crime* merupakan ancaman nyata yang memerlukan penanganan serius melalui kebijakan hukum pidana yang efektif.

Di Indonesia, *cybercrime* telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP) yang menjadi landasan hukum untuk mengatasi *cybercrime* di Indonesia.

Berdasarkan uraian-uraian di atas tujuan dari penelitian ini adalah mengetahui peranan politik hukum dalam penanganan kejahatan siber (*cybercrime*), mengetahui kebijakan hukum pidana dalam penanggulangan *cybercrime*, serta strategi dalam pemberantasan *cybercrime* di Indonesia. Melalui penelitian ini, diharapkan dapat ditemukan solusi yang lebih efektif dalam menangani *cybercrime*, sehingga dapat meningkatkan keamanan digital di Indonesia. Dengan demikian, masyarakat dapat memanfaatkan teknologi informasi dan komunikasi dengan lebih aman, serta meminimalisir dampak negatif dari kejahatan siber terhadap individu, perusahaan, dan negara. Oleh karena itu, Penulis tertarik untuk melakukan penelitian dan menuangkan dalam artikel dengan judul "Kebijakan Hukum Pidana untuk Penanggulangan *Cyber Crime* di Indonesia".

2. METODE PENELITIAN

Penulis menggunakan metode yuridis normatif, yang melibatkan analisis terhadap peraturan perundang-undangan, literatur hukum, dan dokumen terkait lainnya yang relevan dengan kebijakan hukum

[1] https://www.statista.com/topics/11732/cybersecurity-and-cybercrime-in-indonesia/#statisticChapter (diakses pada 11 Juli 2024).

[2]https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf (diakses pada 11 Juli 2024).

pidana dalam penanggulangan kejahatan siber di Indonesia. Metode ini dipilih karena memungkinkan analisis mendalam terhadap aspek hukum yang berlaku. Pendekatan yang digunakan adalah pendekatan konseptual (*conceptual approach*) yang mana digunakan untuk mengkaji konsep-konsep hukum yang terkait. Data dalam penelitian ini dikumpulkan melalui studi pustaka meliputi analisis terhadap peraturan perundang-undangan, putusan pengadilan, jurnal hukum, buku teks, dan dokumen terkait lainnya. Analisis dilakukan dengan menggunakan pendekatan deskriptif analitis, yaitu menggambarkan kebijakan hukum pidana yang ada dan menganalisis efektivitasnya dalam penanggulangan *cybercrime*.

3. PEMBAHASAN

3.1 Peranan Politik Hukum dalam Penanganan Kejahatan Siber (*Cyber Crime*)

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[3]. Peraturan tersebut memerlukan kepastian pengelolaan data dan informasi, khususnya dalam pengelolaan data pribadi, karena tanpa pengelolaan data yang baik dan benar maka akan menimbulkan penyalahgunaan dan serangan *cybercrime*. Oleh karena itu, diperlukan analisis manajemen risiko dalam menghadapi serangan *cybercrime*.[4] Karena serangan *cybercrime* ini berpotensi kehilangan informasi data, permasalahan seperti ini masih sulit untuk diatasi. Kejahatan mengenai data pribadi sering kali ditemukan dalam suatu perusahaan karena dalam hal ini mereka perlu mempelajari bagaimana data tersebut dikelola dan diamankan dengan baik dan benar. Dalam hal ini, perusahaan harus memahami peraturan, prinsip, dan praktik mengenai perlindungan data pribadi. Agar pihak-pihak yang tidak bertanggung jawab tidak menyalahgunakan data dan informasi seseorang.

Meski demikian, belum adanya peraturan mengenai perlindungan data pribadi menyebabkan banyak terjadinya kejahatan penyalahgunaan sistem informasi dan data pribadi. Oleh karena itu diperlukan suatu sistem yang dapat mengatasi hal tersebut. Seperti diketahui, hingga saat ini Indonesia belum memiliki undang-undang yang dapat melindungi data pribadi seseorang. Selama ini masih terdapat tersendiri dalam beberapa peraturan perundang-undangan, sehingga perlu adanya undang-undang yang mengatur secara komprehensif, jelas, dan tegas terkait penyalahgunaan hak milik.

3.2 Kebijakan Hukum Pidana dalam Penanggulangan *Cyber Crime*

Kebijakan pencegahan *cybercrime* dengan hukum pidana mencakup bidang kebijakan penal yang merupakan bagian dari kebijakan kriminal. Dari sudut pandang kebijakan pidana, upaya pencegahan kejahatan (termasuk penanggulangan *cybercrime*) tidak dapat dilakukan hanya secara parsial dengan hukum pidana (hukum pidana) namun hal tersebut juga harus dilakukan dengan pendekatan sistematik[5].

Pada hakikatnya politik atau kebijakan hukum pidana adalah bagaimana hukum pidana dapat dirumuskan secara memadai, memberikan pedoman bagi pembentuk undang-undang, dan melaksanakan hukum pidana. Kebijakan legislatif sangat menentukan dalam tahap-tahap berikutnya karena pada saat akan dibuat peraturan perundang-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 hanya menggugat secara perdata. Selain itu, Pasal 26 UU ITE hanya tentang perlindungan esensial. Pakar teknologi informasi menilai Pasal 26 UU ITE memiliki kelemahan. Kekurangannya adalah tidak adanya perlindungan pengguna yang data pribadinya digunakan untuk memperoleh keuntungan tertentu bagi perusahaan. Keamanan data dimaksudkan untuk meningkatkan keamanan data dan berfungsi untuk 1) Melindungi data agar tidak dapat dibaca oleh orang yang tidak berkepentingan; 2) Mencegah orang yang tidak berkepentingan memasukkan atau menghapus data.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan merupakan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (tindak pidana). Keputusan untuk melakukan kriminalisasi dan dekriminalisasi harus didasarkan pada faktor kebijakan tertentu yang mempertimbangkan berbagai faktor, antara lain 1) Keseimbangan cara yang digunakan sehubungan dengan hasil yang ingin dicapai; 2) Analisis biaya terhadap hasil yang diperoleh mengenai tujuan yang dicari; 3) Penelitian atau penafsiran tujuan yang ingin dicapai mengenai prioritas lain dalam pengalokasian sumber daya manusia; 4) Pengaruh sosial kriminalisasi dan dekriminalisasi berkaitan atau dilihat dari dampak

[3]Haingo Rabarijaona dan Devina Arifani, *Perlindungan Hukum Terhadap Pegawai/Pekerja Yang Mengalami Dampak Digitalisasi Hubungan Kerja*, Jurnal Pembaharuan Hukum, Vol. 7, No.3, 2020, hlm. 211.

[4] Angga Dewanto Basari, Muhammad Syauqillah, dan Asep Usman Ismail, *Kajian Penerapan Aturan Kegiatan Terorisme di Media Sosial*, Jurnal Studi Strategis dan Global, Vol. 3, No. 2, 2020, hlm. 5.

[5] James Popham, Mary McCluskey and Michael Ouellet, *Exploring Police-Reported Cybercrime In Canada Variation And Correlates*, Policing: An International Journal, Vol. 43, No. 1, 2020, hlm. 35.

sekundernya. Dalam mengkriminalisasi suatu perbuatan perlu diperhatikan empat hal sebagai berikut: 1) Penggunaan hukum pidana perlu memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata baik materiil maupun spiritual berdasarkan Pancasila; 2) Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana haruslah perbuatan yang tidak dikehendaki, yaitu perbuatan yang menimbulkan kerugian (baik materiil maupun spirituil) bagi anggota masyarakat; 3) Penggunaan hukum pidana perlu memperhatikan asas biaya dan manfaat; 4) Penggunaan hukum pidana juga harus memperhatikan kapasitas atau daya kerja lembaga penegak hukum pidana sehingga sehingga tidak terjadi beban tugas yang berlebihan[6].

Kebijakan kriminalisasi atau rumusan hukum pidana di Indonesia terkait permasalahan *cybercrime* selama ini dapat diidentifikasi sebagai berikut:

a) Dalam KUHP

Rumusan tindak pidana dalam KUHP sebagian besar masih konvensional dan belum berkaitan langsung dengan perkembangan *cybercrime*. Selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan kejahatan teknologi tinggi yang sangat bervariasi. Misalnya, KUHP kesulitan menangani pemalsuan kartu kredit dan transfer dana elektronik karena tidak ada aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya menyangkut: a) sumpah/pernyataan palsu (Pasal 242); b) menghindari mata uang dan uang kertas (Pasal 244-252); c) pemalsuan stempel dan tanda (Pasal 253-262); dan (d) pemalsuan surat (Pasal 263-276)[7].

b) Undang-undang di luar KUHP

1. Undang-Undang No.36 Tahun 1999 tentang Telekomunikasi mengancam tindak pidana terhadap a) Memanipulasi akses ke jaringan telekomunikasi (Pasal 50 jo. Pasal 22); b) Mengakibatkan gangguan fisik dan elektromagnetik pada penyelenggaraan telekomunikasi (Pasal 55 jo. Pasal 38); c) Melakukan penyadapan atas informasi melalui jaringan telekomunikasi (Pasal 56 jo. Pasal 40);
2. Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang; dan Pasal 44 ayat (2) UU No. 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi, mengakui rekaman elektronik sebagai alat bukti yang sah;

c) Undang-Undang No. 32 Tahun 2002 tentang Penyiaran, antara lain mengatur tentang tindak pidana: 1) Pasal 57 jo. 36 ayat (5) mengancam pidana terhadap siaran yang: a) bersifat fitnah, menghasut, menyesatkan, atau bohong; b) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau c) mempertentangkan suku, agama, ras, dan antargolongan; 2) Pasal 57 jo. Pasal 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan, melecehkan, atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional; 3) Pasal 58 jo. 46 ayat (3) mengancam pidana siaran iklan niaga yang memuat: a) promosi yang berhubungan dengan ajaran suatu agama, ideologi, perseorangan, atau kelompok, yang menyinggung perasaan atau merendahkan martabat orang lain, ideologi lain, perseorangan lain, atau kelompok lain; b) promosi minuman keras atau sejenisnya serta zat atau bahan yang bersifat adiktif; c) promosi rokok yang memperagakan wujud rokok; d) hal-hal yang bertentangan dengan kesusilaan dan nilai-nilai agama; atau e) eksploitasi anak di bawah umur[8];

d) Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE), memuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan 1) Melanggar kesusilaan; memiliki muatan perjudian; mengandung penghinaan atau pencemaran nama baik; memiliki muatan pemerasan atau pengancaman (Pasal 27); 2) Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik; menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) (Pasal 28); 3) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan

[6] Sri Hartati, Hadi Karyono, dan Hudi Karno Sabowo, *Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia*, International Journal of Educational Research & Social Sciences, Vol. 3, No. 1, 2022, hlm.425.

[7] Nurianto Rachmad Soepadmo, *Impact Analysis of Information and Electronic Transactions Law (Law No. 19 Year 2016) on the Level of Cyber-Crime in Social Media*, International Journal of Innovation, Creativity and Change, Vol. 12, No. 8, 2020, hlm. 490.

[8] Muhammad Isnaeni Puspito Adhi and Eko Soponyono, *Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law*, Law Reform, Vol. 17, No. 2, 2021, hlm. 140.

secara pribadi (Pasal 29); 3) Mengakses komputer atau sistem elektronik milik orang lain; mengakses komputer atau sistem elektronik dengan tujuan untuk memperoleh informasi elektronik atau dokumen elektronik; mengakses komputer atau sistem elektronik dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30); 4) Melakukan intersepsi atau penyadapan atas informasi elektronik atau dokumen elektronik; melakukan intersepsi secara elektronik atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik (Pasal 31); 5) Melakukan penyadapan atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik (Pasal 32); 6) Melakukan penyadapan atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik (Pasal 33); 7) Melakukan penyadapan atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik (Pasal 31); Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki a) perangkat keras atau perangkat lunak yang dirancang atau dibuat khusus untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27-33; b) kata sandi melalui komputer, kode akses, atau hal lain yang sejenis yang dimaksudkan agar sistem elektronik dapat diakses untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27-33 (Pasal 34); 8) Memanipulasi, melakukan penciptaan, perubahan, penghilangan, dan pengrusakan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35); 9) Melakukan perbuatan sebagaimana dimaksud dalam Pasal 27-34 yang menyebabkan kerugian bagi orang lain (Pasal 36); 10) Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27-36 di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah Yurisdiksi Indonesia (Pasal 37); 11) Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27-36 di dalam wilayah Yurisdiksi Indonesia (Pasal 38). yang berada di wilayah Yurisdiksi Indonesia (Pasal 37).[9]

Kriminalisasi *cybercrime* di Indonesia, khususnya dalam UU ITE, dapat dibagi menjadi dua kategori, yaitu tindakan yang menggunakan komputer sebagai sarana kejahatan dan tindakan yang menjadikan komputer sebagai target kejahatan. Kejahatan yang menggunakan komputer sebagai sarana segala perbuatan yang memanfaatkan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di dunia maya, bukan di dunia nyata.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet). Aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusi penegak hukum di daerah yang belum didukung dengan jaringan Internet.[10]

3.3 Strategi dalam Pemberantasan *Cyber Crime* di Indonesia

Dalam menanggulangi *cybercrime* 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[11]. Dengan demikian maka penanggulangan kejahatan lebih baik dilakukan dengan menggunakan kebijakan non penal yang bersifat preventif. Kebijakan dalam penanggulangan *cybercrime* dapat dilakukan dengan dua acara 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 memberantas *cybercrime.*

[9] Sri Hartati, Hadi Karyono, and Hudi Karno Sabowo, *Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia*, International Journal of Educational Research & Social Sciences, Vol. 3, No. 1, 2022, hlm. 430.

[10] Andhika Abdillah, Muhammad Muhtarom, Ismiyanto, *Kebijakan Penanggulangan Kejahatan Tindak Pidana Teknologi Informasi,* Journal UNIBA, Vol. 34 No. 02, 2022, hlm. 14.

[11] Hatta, *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan*, Pustaka Pelajar, Yogyakarta, 2010, hlm. 39.

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[12]:

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 di tempat 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. Kerjasama internasional dalam penanggulangan *cybercrime* sangat diperlukan mengingat *cybercrime* merupakan kejahatan transnasional yang terorganisir.

4. KESIMPULAN DAN SARAN/REKOMENDASI

4.1 Kesimpulan

Politik hukum memiliki peran penting dalam proses pembaharuan hukum untuk mengimbangi perkembangan zaman yang begitu cepat. Pembaharuan hukum tersebut mencerminkan upaya untuk mewujudkan amanat alinea keempat UUD 1945 dan ketentuan-ketentuan lain yang terkandung di dalamnya. Dalam menghadapi perubahan sosial, ketika terjadi perubahan pola perilaku hukum, maka dipedomani untuk menjadi pedoman dalam mengatur masyarakat. Hukum harus mengikuti konsideran dari awal pembentukan UU ITE dan revisi UU ITE. Dan penegakan hukum juga memperhatikan penerapan asas keadilan, kesetaraan, dan kepastian hukum karena untuk saat ini Undang-Undang Informasi dan Transaksi Elektronik dibentuk mengikuti kemauan politik dan perkembangan yang isi dan penafsirannya lebih berpihak kepada pemerintah dan membatasi hak-hak masyarakat Indonesia.

4.2 Saran/Rekomendasi

Perlu adanya revisi dan pembaharuan Undang-Undang ITE (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP) untuk mengakomodasi perkembangan teknologi dan ancaman baru dalam cybercrime. Mengingat pentingnya kesadaran akan keamanan siber, diperlukan kampanye edukasi secara luas kepada masyarakat tentang potensi risiko cybercrime dan cara-cara untuk melindungi diri mereka. Ini dapat dilakukan melalui program-program pendidikan formal dan informal serta kampanye media sosial. Selanjutnya, Diperlukan investasi dalam infrastruktur keamanan siber dan peningkatan jumlah serta kualitas tenaga ahli keamanan siber di Indonesia. Ini mencakup pendidikan dan pelatihan yang lebih baik bagi aparat penegak hukum dan profesional teknologi informasi untuk mengatasi kejahatan siber dengan lebih efektif.

REFERENSI

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

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

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

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

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

[12] Soejadi, *Refleksi Mengenai hukum dan Keadilan: Aktualisasinya di Indonesia*, Aswaja Pressindo, Yogyakarta, 2017, hlm. 56.

Hatta. (20210). *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan.* Yogyakarta: Pustaka Pelajar.

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

Rabarijaona, H., & Arifani, D. (2020). Perlindungan Hukum Terhadap Pegawai/Pekerja Yang Mengalami Dampak Digitalisasi Hubungan Kerja. *Jurnal Pembaharuan Hukum, 7*(3).

Soejadi. (2017). *Refleksi Mengenai hukum dan Keadilan: Aktualisasinya di Indonesia, Aswaja Pressindo.* Yogyakarta: Aswaja Pressindo.

Soepadmo, N. R. (2020). Impact Analysis of Information and Electronic Transactions Law (Law No. 19 Year 2016) on the Level of Cyber-Crime in Social Media. *International Journal of Innovation, Creativity and Change, 12*(8).

https://www.statista.com/topics/11732/cybersecurity-and-cybercrime-in-indonesia/#statisticChapter

https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf