Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia

Adji Saputra[1*], **Kristiawanto**[2], **Mohamad Ismed**[3]
[1,2,3]Program Studi Magister Ilmu Hukum, Pascasarjana Universitas Jayabaya
2021010262007@pascajayabaya.ac.id[*]

SEIKAT
Jurnal Ilmu Sosial, Politik dan Hukum

e-ISSN: 2964-0962

SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum

https://ejournal.45mataram.ac.id/index.php/seikat

Vol. 3 No. 1 Februari 2024

Page: 63-70

Available at:

https://ejournal.45mataram.ac.id/index.php/seikat/article/view/1186

DOI:

https://doi.org/10.55681/seikat.v3i1.1186

Article History:

Received: 02-02-2024

Revised: 07-02-2024

Accepted: 08-02-2024

Abstract *: The threat of cybercrime in the era of digital transformation is the main focus of society, continuing to grow along with the ease and challenges brought by the transformation. Cybercrime uses digital technology, causing material and non-material harm to individuals, organizations and the state. The method used is juridical normative by using primary, secondary and tertiary sources of legal materials. Collection techniques of legislation and conceptual analytical and legal material carried out by identifying and inventorying positive legal rules, researching library materials and other sources of legal materials that are relevant to the legal issues under study. The result of this study is that cybercriminals in the era of digital transformation in Indonesia pose a serious threat, especially in the economic field. The sustainability of advances in digital technology carries significant adverse impacts, including financial losses, social disruption, and even threats to national security stability. Law enforcement against cybercrime requires national attention and vigilance, with a focus on improving information technology security, cybersecurity literacy, establishing effective regulations, and cooperation between governments, security authorities, and the public. These measures are key in anticipating and preventing the worse impact of cybercrime on the economy.*

Keywords *: Law Enforcement; Cybercrime; Digital Transformation*

Abstrak : Ancaman kejahatan siber di era transformasi digital menjadi fokus utama masyarakat, terus berkembang seiring kemudahan dan tantangan yang dibawa oleh transformasi tersebut. Kejahatan siber menggunakan teknologi digital, merugikan materiil dan non-materiil bagi individu, organisasi, dan negara. Metode yang digunakan adalah Yuridis normatif dengan menggunakan sumber bahan hukum primer, sekunder dan tersier. Teknik pengumpulan materi perundang-undangan dan konseptual analitis serta hukum yang dilakukan dengan mengidentifikasi dan menginventarisasi kaidah-kaidah hukum yang positif, meneliti bahan pustaka dan sumber bahan hukum lainnya yang relevan dengan permasalahan hukum yang diteliti. Hasil dari penelitian ini adalah bahwa Pelaku kejahatan siber di era transformasi digital di Indonesia menimbulkan ancaman serius, terutama dalam bidang ekonomi. Keberlanjutan kemajuan teknologi digital membawa dampak merugikan yang signifikan, mencakup kerugian keuangan, gangguan sosial, dan bahkan ancaman terhadap stabilitas keamanan nasional. Penegakan hukum terhadap kejahatan siber memerlukan perhatian dan kewaspadaan nasional, dengan fokus pada peningkatan keamanan teknologi informasi, literasi keamanan siber, pembentukan regulasi efektif, serta kerjasama antara pemerintah, otoritas keamanan, dan masyarakat. Langkah-langkah tersebut menjadi kunci dalam mengantisipasi dan mencegah dampak yang lebih buruk akibat kejahatan siber di bidang ekonomi.

Kata Kunci : Penegakan Hukum; Tindak Pidana Siber; Transformasi Digital

PENDAHULUAN

Tindak pidana siber atau kejahatan dunia maya semakin menjadi perhatian utama di Indonesia seiring dengan perkembangan teknologi informasi dan komunikasi. Rekonstruksi penegakan hukum terhadap tindak pidana siber di Indonesia melibatkan berbagai aspek, mulai dari peraturan hukum, lembaga penegak hukum, hingga kerjasama internasional (Rahardjo, 1987).

Pengaruh transformasi digital yang pesat di Indonesia menuntut sebuah rekonstruksi mendalam dalam penegakan hukum terhadap tindak pidana siber. Dalam era ini, keamanan nasional, khususnya di sektor ekonomi, semakin terancam oleh pelaku kejahatan siber yang semakin canggih. Dampaknya tidak hanya bersifat finansial, melainkan juga mencakup gangguan sosial dan ancaman terhadap stabilitas keamanan nasional (Widodo, 2011).

Dalam konteks ini, rekonstruksi penegakan hukum menjadi sebuah keharusan. Faktor-faktor seperti kemajuan teknologi, kompleksitas ekonomi digital, dan perubahan paradigma kejahatan siber menuntut perubahan mendasar dalam pendekatan penegakan hukum di Indonesia. Urgensi rekonstruksi ini tergambar dari tingginya tingkat kerugian yang dihasilkan oleh tindak pidana siber, mencakup kerugian finansial yang substansial, gangguan aktivitas bisnis, serta ancaman terhadap keamanan nasional. Pada tahun 2016, Indonesia mengesahkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini menjadi landasan hukum utama dalam penanganan tindak pidana siber di Indonesia. Selain itu, terdapat juga regulasi lain yang mendukung penegakan hukum terhadap kejahatan dunia maya, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Maramis, 2016).

Penegakan hukum terhadap tindak pidana siber di Indonesia melibatkan berbagai lembaga, antara lain Kepolisian Republik Indonesia (POLRI), Kejaksaan Agung, dan Komisi Pemberantasan Korupsi (KPK). POLRI memiliki satuan khusus yang fokus menangani kejahatan dunia maya, yaitu Direktorat Tindak Pidana Siber Bareskrim Polri. Selain itu, Kejaksaan Agung juga memiliki peran penting dalam penuntutan pelaku kejahatan siber.

Dalam era globalisasi dan konektivitas yang tinggi, kerjasama internasional menjadi hal yang krusial dalam penanganan tindak pidana siber. Indonesia aktif melakukan kerjasama dengan negara-negara lain dalam hal pertukaran informasi dan bukti elektronik, pelatihan penegakan hukum terkait kejahatan dunia maya, serta pengembangan regulasi bersama.

Rekonstruksi penegakan hukum terhadap tindak pidana siber mencakup beberapa dimensi utama. Pertama, peningkatan keamanan teknologi informasi menjadi suatu keharusan. Ini melibatkan penguatan sistem keamanan siber untuk melindungi infrastruktur kritis dan data sensitif. Kedua, literasi keamanan siber di kalangan masyarakat perlu ditingkatkan agar dapat merespon ancaman digital dengan bijak. Selanjutnya, kolaborasi aktif antara pemerintah, otoritas keamanan, dan masyarakat menjadi esensial dalam menghadapi kompleksitas kejahatan siber. Pembentukan kebijakan dan regulasi yang responsif terhadap dinamika tindak pidana siber menjadi langkah kunci. Kebijakan ini harus dapat mengakomodasi perkembangan teknologi, mendukung penegakan hukum yang efektif, dan melibatkan partisipasi masyarakat dalam upaya pencegahan (McGregor, 1995).

Dengan adanya rekonstruksi penegakan hukum terhadap tindak pidana siber di Indonesia melalui peraturan hukum yang memadai, peran lembaga penegak hukum yang profesional, serta kerjasama internasional yang solid, diharapkan dapat meningkatkan efektivitas dalam menangani kejahatan dunia maya demi terciptanya lingkungan digital yang aman dan terpercaya bagi masyarakat. Langkah-langkah konkret dalam rekonstruksi ini mencakup pendirian tim yang terlatih dalam operasi militer *cyber warfare*, pemantauan aktif terhadap serangan siber, serta penanganan cepat atas tindak pidana siber. Peningkatan kapabilitas penegakan hukum, baik dari segi teknis maupun personel, menjadi bagian integral dari rekonstruksi ini.

METODE PENELITIAN

Menurut (Ramlani Lina S, 2021) Penelitian (*research*) sesuai dengan tujuannya dapat didefinisikan sebagai usaha untuk menemukan, mengembangkan dan menguji kebenaran suatu pengetahuan. Penelitian dilakukan dengan menggunakan metode-metode ilmiah yang disebut dengan metodologi penelitian. Jenis penelitian yang digunakan adalah metode penelitian hukum normatif melalui data empiris dalam mengkaji dan menganalisis permasalahan hukum atas peraturan Perundang-Undangan yang berlaku (Marzuki, Penelitian Hukum, 2005). Teknik pengumpulan data yang dipergunakan melalui studi kepustakaan. Teknik Pengumpulan Bahan Hukum pada penelitian normatif dibatasi pada penggunaan studi dokumen atau bahan pustaka saja yaitu pada data hukum sekunder (Mamudji, 2009).

HASIL DAN PEMBAHASAN

Peneliti terdiri dari dua analisis yakni Analisis tentang penegakan hukum tindak pidana siber di era transformasi digital di Indonesia saat ini dan rekonstruksi konsep penegakan hukum tindak pidana siber di Indonesia ke depan.

Penegakan Hukum Tindak Pidana Siber di Era Transformasi Digital di Indonesia Saat Ini

Pelaku tindak pidana siber di Indonesia saat ini menjadi ancaman serius, khususnya dalam bidang ekonomi, memerlukan perhatian dan kewaspadaan nasional. Dalam era digitalisasi, ekonomi Indonesia semakin rentan terhadap serangan tindak pidana siber, seperti perbankan, pencurian data nasabah, penipuan online, dan perdagangan ilegal. Dampak dari serangan ini dapat merugikan masyarakat secara luas, mengancam keamanan nasional, dan membawa risiko signifikan pada pertumbuhan ekonomi.

Dalam upaya penegakan hukum terhadap tindak pidana siber, beberapa tantangan muncul, terutama dalam harmonisasi regulasi terkait penggunaan atau melalui internet. Praktek penanganan terhadap tindak pidana penipuan, perjudian, dan pornografi masih menggunakan ketentuan dalam KUHP. Meskipun demikian, penggunaan teknologi informasi dan komunikasi terus berkembang, mengubah cara transaksi, berbelanja, berinvestasi, dan beroperasi dalam bisnis. Namun, perkembangan ini juga membuka peluang bagi kejahatan siber, seperti serangan terhadap perbankan, pencurian data, dan perdagangan ilegal.

Langkah-langkah konkret dalam melindungi sistem komputer, jaringan, perangkat elektronik, dan data dari ancaman siber menjadi penting. Keamanan siber bertujuan menjaga kerahasiaan, integritas, dan ketersediaan informasi yang sensitif, serta melindungi infrastruktur teknologi informasi dari serangan yang dapat merusak sistem atau menyebabkan kerugian yang signifikan.

Dalam upaya bersama melindungi keamanan dan kedaulatan negara dari potensi ancaman dan gangguan, kolaborasi antara pemerintah, sektor swasta, dan masyarakat semakin diperkuat. Program pendidikan dan pelatihan keamanan siber ditingkatkan untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman siber. Meskipun demikian, tingkat kejahatan siber terus berkembang dan semakin kompleks.

Selain itu, fenomena cyberbullying melalui media sosial menjadi perhatian serius, terutama dalam penghormatan terhadap kebebasan berekspresi dan perlindungan terhadap korban. Pelaksanaan penegakan hukum pidana terhadap cyberbullying perlu mempertimbangkan delik aduan yang melibatkan perbuatan seperti body shaming, penghinaan, pencemaran nama baik, dan ancaman.

Pemerintah Indonesia telah merespons peningkatan ancaman kejahatan siber dengan adopsi kebijakan dan regulasi yang bertujuan untuk meningkatkan keamanan siber dan melindungi infrastruktur informasi kritikal. Pendirian Badan Siber dan Sandi Negara (BSSN) merupakan langkah konkret pemerintah dalam menghadapi ancaman ini. Kendati demikian, tantangan tetap ada, dan pembaruan terus-menerus dalam regulasi dan peningkatan kapabilitas penegakan hukum diperlukan untuk menjaga keamanan nasional dan meminimalkan risiko kejahatan siber di Indonesia.

Kemajuan teknologi informasi internet segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri dimana semakin mudahnya para pelaku kejahatan melakukan aksinya yang semakin merisaukan masyarakat. Penyalahgunaan yang terjadi dalam *cyber space*

inilah yang dikenal dengan *cyber crime.* Walaupun kejahatan dunia maya atau kejahatan siber umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Fungsi sanksi dalam hukum pidana, tidak semata-mata menakut-nakuti atau mengancam para pelanggar, keberadaan sanksi tersebut juga harus dapat mendidik dan memperbaiki pelaku. Berkembangnya konsep untuk mencari alternatif dari pidana perampasan kemerdekaan *alternative to imprisonment* dalam bentuknya sebagai sanksi alternatif *alternative sanction* (Saleh, 2013).

Rudolph B. Schesinger perbandingan hukum merupakan metode penyelidikan dengan tujuan untuk memperoleh pengetahuan yang lebih dalam tentang bahan-bahan hukum tertentu. Perbandingan hukum bukanlah perangkat peraturan dan asas-asas hukum dan bukan suatu cabang hukum, melainkan merupakan teknik untuk menghadapi unsur hukum asing dari suatu masalah hukum (Kristiawanto, 2021).

Munir Fuady, mendefinisikan perbandingan hukum sebagai pengetahuan dan metode mempelajari ilmu hukum dengan meninjau lebih dari satu sistem hukum dengan meninjau kaidah dan atau aturan hukum dan atau yurisprudensi serta pendapat ahli yang kompeten dalam berbagai sistem hukum tersebut, untuk menemukan persamaan dan perbedaan sehingga dapat ditarik kesimpulan dan konsep tertentu, dan menemukan penyebab timbulnya persamaan dan perbedaan tersebut, baik secara historis, sosiologis, analitis maupun normatif.

Berdasarkan ketentuan dalam Pasal 5 KUHP hukum pidana Indonesia berlaku terhadap setiap warga negara Indonesia yang di luar wilayah Indonesia melakukan tindak pidana tertentu yaitu:

1. Tindak pidana terhadap keamanan negara (Pasal 104-Pasal 129 KUHP).
2. Tindak pidana terhadap Martabat Presiden dan Wakil Presiden (Pasal 130-Pasal 139 KUHP).
3. Tindak Pidana menghasut melakukan tindak pidana (Pasal 160 KUHP).
4. Tindak pidana menyiarkan tulisan yang bertujuan menghasut (Pasal 161 KUHP).
5. Tindak pidana dengan sengaja membuat diri sendiri atau orang lain tidak mampu untuk memenuhi kewajiban militer (Pasal 240 KUHP).
6. Tindak pidana mengadakan perkawinan padahal mengetahui perkawinan yang ada menjadi penghalang yang sah untuk itu (Pasal 279).
7. Tindak pidana pembajakan di laut (Pasal 450 dan Pasal 451 KUHP).
8. Tindak pidana yang menurut Undang-Undang Pidana Indonesia dipandang sebagai kejahatan dan menurut negara tempat tindak pidana dilakukan diancam dengan pidana (suseno, 2012).

Hukum yang berlaku di Indonesia adalah Hukum yang berasal dari aturan-aturan Hukum negara Belanda, sebab untuk membuat aturan Hukum membutuhkan waktu yang panjang dan akan melibatkan seluruh elemen masyarakat di Indonesia. Penerapan Hukum di Indonesia banyak bersumber dari undang-undang atau aturan-aturan yang berasal dari Hukum Belanda, namun seiring perkembangan zaman tak hanya dilakukan revisi untuk menyesuaikan dengan perilaku kehidupan masyarakat indonesia.

Dalam Undang-Undang No. 44 Tahun 2008 tentang Pornografi juga terdapat tindak pidana yang termasuk tindak pidana siber. Hal ini berkaitan dengan pengertian ponografi dalam ketentuan Umum Pasal 1 ayat 1 diperluas tidak hanya dalam bentuk cetak tetapi juga dalam berbagai bentuk media komunikasi termasuk internet. Demikian pula dalam pengertian jasa pornografi (Pasal 1 angka 2) termasuk didalamnya layanan melalui internet dan komunikasi elektronik lainnya.

Berdasarkan pengertian tersebut maka kriminalisasi perbuatan dalam Undang-Undang Pornografi dapat ditafsirkan termasuk juga perbuatan yang dilakukan dengan melalui teknologi informasi dan komunikasi. Ada beberapa perbuatan yang dikriminalisasi dalam undang undang pornografi yaitu :

1. Memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit.

2. Subtansi yang didalamnya mengandung sistem Hukum pidana materiil beserta asasasas Hukum pidana yang mendasarinya, disusun dan diformulasikan, dengan berorientasi pada berbagai pokok pemikiran dan ide dasar keseimbangan, antara lain mencakup Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU KUHP).
3. Keseimbangan antara moralitas yang berkaitan dengan kepentingan Negara, kepentingan umum masyarakat dan kepentingan individu perorangan.
4. Keseimbangan antara perlindungan terhadap kepentingan publik, kepentingan pelaku tindak pidana,dan kepentingan korban tindak pidana.
5. Keseimbangan antara unsur, faktor objektif, dan subjektif.
6. Keseimbangan antara kriteria formal dan materiil.
7. Keseimbangan antara kepastian Hukum, kelenturan elastisitas atau fleksibilitas dan keadilan. Keenam, keseimbangan antara kearifan local kearifan faltikuralistik, nilai-nilai nasional dan nilai-nilai global (Bakhri, 2011).

Indonesia belum mempunyai hukum special atau *cyber law* yang menata hal *cyber crime*, ada Sebagian hukum positif lain yang legal biasa serta bisa dikenakan untuk para pelakon *cyber crime* paling utama buat kasus memakai komputer dan lainya (Setiawan, 2005). Penguatan hukum kepada seorang yang sudah melaksanakan aksi kejahatan namun tidak bisa dipertanggung jawabkan sebab dalam Pasal 44 buku hukum kejahatan itu, sehingga bukanlah dipidana. Bagi Martiman Prodjohamidjojo seorang memperoleh kejahatan terkait pada 2 perihal:

1. Wajib terdapat aksi yang berlawanan dengan hukum, ataupun dengan tutur lain wajib terdapat faktor melawan dengan hukum.
2. Kepada pelakunya terdapat faktor kekeliruan dalam wujud kesengajaan ataupun kealpaan, aksi yang melanggar hukum bisa dipertanggung jawabkan jadi faktor individual (Prodjohamidjojo, 1996).

Subyek hukum selaku pelakon perbuatan kejahatan *Cyber Crime* senantiasa diamati dari keahlian bertanggung jawab. Pertanggung jawaban kejahatan terdiri serta dua pertanggung jawabkan serta kejahatan. Pertanggung jawaban berawal serta tutur bawah tanggung jawab. Bagi W.J.S. Poerwadarminta tanggung jawab dimaksudkan selaku kondisi harus menanggung seluruh sesuatunya terdapat bisa dituntut, dipersalahkan, diperkarakan serta separuhnya (Poerwadarminta, 1996).

Urgensi hukum pidana siber dari analisis ini adalah mencakup perlunya penegakan hukum yang efektif dan responsif terhadap kejahatan siber di tengah transformasi digital. Dalam era ini, kehadiran hukum pidana siber menjadi krusial untuk melindungi masyarakat dan instansi dari ancaman kejahatan di dunia maya. Hal ini mencakup penanganan serius terhadap pencurian data, penipuan online, dan ancaman siber lainnya yang dapat merugikan individu, organisasi, serta mengancam keamanan nasional. Kesinambungan penegakan hukum dalam konteks digital sangat penting untuk menjaga ketertiban dan keadilan di tengah dinamika teknologi yang terus berkembang.

Rekonstruksi Konsep Penegakan Hukum Tindak Pidana Siber di Indonesia Ke Depan

Rekonstruksi konsep penegakan hukum terhadap tindak pidana siber di Indonesia ke depan menjadi suatu keharusan dalam menghadapi tantangan yang semakin kompleks di era digital. Seiring dengan kemajuan teknologi, kejahatan siber semakin berkembang dan menghadirkan risiko baru bagi masyarakat dan pemerintah. Dalam rekonstruksi konsep penegakan hukum, perlu dipertimbangkan peningkatan kapasitas hukum untuk mengantisipasi dan menanggapi metode kejahatan siber yang terus berkembang. Upaya ini harus melibatkan kerjasama antara lembaga penegak hukum, sektor swasta, dan pihak-pihak terkait lainnya. Selain itu, penyusunan regulasi yang lebih presisi dan adaptif terhadap dinamika kejahatan siber menjadi kunci dalam menjaga keamanan siber dan melindungi masyarakat. Melalui rekonstruksi ini, diharapkan penegakan hukum tindak pidana siber dapat lebih efektif, responsif, dan mampu mengimbangi perkembangan teknologi untuk menjaga kestabilan dan keamanan di ranah digital di Indonesia.

Konsep penegakan hukum tindak pidana siber di Indonesia dalam Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran. Di samping terdapat perlindungan hukum, disana

juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan. Tindak pidana peretasan yang diatur dalam pasal 30 ayat (1),(2),dan (3) mengandung unsur sebagai berikut.

Pasal 30 ayat (1) UU ITE setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan sistem elektronik milik orang lain dengan cara apapun. Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses komputer dan sistem elektronik milik orang lain, serta unsur dengan cara apapun.

1. Unsur setiap orang dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggung jawab dan cakap hukum berdasarkan atas Perundang-Undangan.
2. Unsur dengan sengaja dan tanpa hak melawan hukum Unsur ini merujuk pada niat atau kesengajaan dan penuh dengan keasadaran dari orang tesebut dalam melakukan suatu tindakan yang malawan hukum.
3. Unsur mengakses komputer dan sistem elektronik milik orang lain Unsur ini memberi gambaran bahwa sistem elektronik milik orang lain itu berarti hal yang bersifat pribadi milik orang lain dan bukan bersifat untuk umum.
4. Unsur dengan cara apapun Dengan cara apapun yang dimaksud dalam hal ini adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.

Ditinjau dari aspek kelembagaan saat ini di Indonesia Kepolisian daerah yang meiliki unit *Cybercrime* adalah Polda Metro Jaya dan Polda Jawa Timur dan berada dibawah Direktorat Reserse Kriminal, sedangkan penanganannya disamakan dengan kasus-kasus tindak pidana lainya. Data mengenai tindak pidana siber diperoleh dari Polda Sumatra Utara, Polda Jawa Barat, dan Polda Jawa Timur.

Beberapa alasan mengapa statistik tindak pidana siber tidak menggambarkan luas lingkup yaitu:

1. Kecepatan operasional dan kapasitas penyimpanan perangkat komputer membuat tindak pidana untuk dideteksi.
2. Aparat penegak hukum seringkali tidak memiliki keahlian teknis diperlukan untuk menangani tindak pidana yang terjadi dalam lingkungan pengolahan data.
3. Banyak korban kejahatan komputer telah gagal membuat rencana yang memungkinkan menangani kejahatan komputer.
4. Sekali tindak pidana telah terdeteksi, banyak perusahaan enggan untuk melaporkan tindak pidana tersebut karena takut terjadinya publisitas yang merugikan, kehilangan googwill, malu, hilangnya kepercayaan public, kehilangan investor, atau dampak ekonomi.

Rumusan Pasal 28 ayat (1) tidak termasuk *internet fraud* atau *computer related fraud*, karena tidak disyaratkan adanya unsur pokok dalam penipuan, yaitu perbuatan rangkaian kebohongan, tipu muslihat, dll yang mengakibatkan seseorang menyerahkan barang sesuatu kepada dirinya atau orang lain. Unsur kerugian dalam penipuan harus dianggap selalu ada karena tindak pidana penipuan termasuk tindak pidana terhadap kekayaan orang sehingga setiap penipuan harus dianggap merugikan kekayaan orang lain (Prodjodikoro, 2003).

Mengalami situasi begitu, terdapat kegagalan serta inovasi dari petugas penegak hukum buat memaksimalkan peraturan yang terdapat dengan melaksanakan interprestasi ataupun arsitektur hukum yang berasal pada filosofi atau ilmu hukum, opini para pakar, yurisprudensi, ataupun berasal dari gagasan bawah yang dengan cara abstrak bisa dipertanggung jawabkan kejahatan memiliki arti pencelaan individual. Maksudnya, dengan cara individual ataupun dipersalahkan atau dipertanggung jawabkan atas perbuatan kejahatan yang dikerjakannya pantas dipidana (Arif, 2005).

Cyber Crime diuraikan oleh beberapa ahli, Andi Hamzah dalam bukunya aspek-aspek pidana di bidang komputer mengartikan *Cyber Crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal. Forester dan Morrison mendefinisikan kejahatan komputer sebagai aksi criminal Dimana komputer digunakan sebagai senjata utama. Girasa Mendefinisikan *Cyber Crime* sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama. Tavani memberikan definisi *Cyber Crime* yang lebih

menarik, yaitu kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber.*

Dalam Undang-Undang No. 19 Tahun 2016 tentang perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirumuskan bahwa:

1. Pasal 32 ayat (2)

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan Dokumen Elektronik milik Orang lain atau milik publik.
2. Pasal 35

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
3. Pasal 48 ayat (2)

   Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
4. Pasal 51 ayat (1)

   Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah) (Hamzah, 2005).

Kejahatan carding dalam hukum pidana diatur dalam Undang-Undang Republik Indonesia No.19 tahun 2016 tentang perubahan atas Undang-Undang Republik Indonesia No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, juga terdapat Pasal-Pasal seperti penipuan yang berkaitan dengan komputer, tindakkan membantu serta kerjasama internasional belum diatur di dalamnya.

Undang-Undang tentang Informatika dan Transaksi Elektronik tersebut, Menghindari multitafsir ketentuan larangan mendistribusikan, mentransmisikan dan membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan pencemaran nama baik pada ketentuan Pasal 27 Ayat (3), dilakukan 3 (tiga) perubahan sebagai berikut :

1. Menambahkan penjelasan atas istilah mendistribusikan, mentransmisikan dan membuat dapat diaksesnya Informasi Elektronik.
2. Menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum.
3. Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) disampaikan kepada DPR RI sebelum disahkan. UU ITE diundangkan pada 21 April 2008 dan menjadi *cyber law* pertama di Indonesia.

Menurunkan ancaman pidana pada 2 (dua) ketentuan sebagai berikut:

1. Ancaman pidana penghinaan dan pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi paling lama 4 (tahun) dan denda dari paling banyak Rp1 miliar menjadi paling banyak Rp750 juta.
2. Ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut nakuti dari pidana penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan denda dari paling banyak Rp2 miliar menjadi paling banyak Rp750 juta.

Urgensi hukum dari analisis ini terletak pada perlunya pemikiran dan perubahan dalam konsep penegakan hukum terhadap kejahatan siber di masa depan. Melalui rekonstruksi ini, dibutuhkan adaptasi hukum yang responsif terhadap perkembangan teknologi dan dinamika kejahatan siber. Hal ini penting untuk menjaga keamanan nasional, melindungi masyarakat, serta memastikan bahwa sistem hukum mampu mengatasi tantangan baru yang muncul seiring dengan kemajuan teknologi informasi dan komunikasi.

KESIMPULAN DAN SARAN

Bahwa Pelaku kejahatan siber di era transformasi digital di Indonesia menimbulkan ancaman serius, terutama dalam bidang ekonomi. Keberlanjutan kemajuan teknologi digital membawa dampak merugikan yang signifikan, mencakup kerugian keuangan, gangguan sosial, dan bahkan ancaman terhadap stabilitas keamanan nasional. Penegakan hukum terhadap kejahatan siber memerlukan perhatian dan kewaspadaan nasional, dengan fokus pada peningkatan keamanan teknologi informasi, literasi keamanan siber, pembentukan regulasi efektif, serta kerjasama antara pemerintah, otoritas keamanan, dan masyarakat. Langkah-langkah tersebut menjadi kunci dalam mengantisipasi dan mencegah dampak yang lebih buruk akibat kejahatan siber di bidang ekonomi.

Sebagai saran Pelaku kejahatan siber di Indonesia memanfaatkan kemajuan teknologi digital. Meskipun teknologi membawa kemudahan transaksi dan berbisnis, semakin luasnya penggunaan teknologi juga meningkatkan risiko serangan kejahatan siber. Ancaman terbesar terjadi dalam bidang ekonomi, termasuk perbankan, pencurian data, penipuan *online*, perdagangan ilegal, serta serangan pada infrastruktur finansial dan pembayaran digital. Dampaknya merugikan individu, perusahaan, dan masyarakat secara keseluruhan, mempengaruhi ekonomi nasional. Perlu peningkatan konsep penegakan hukum terhadap kejahatan siber, khususnya untuk mengatasi pelanggaran di media sosial, sambil terus memahami dan beradaptasi dengan perkembangan teknologi yang semakin canggih.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh tenaga pendidik dan tenaga kependidikan Prodi Magister Ilmu Hukum Program Pascasarjana Universitas Jayabaya yang telah selalu men*support* baik secara moral maupun material selama penulis menyusun penelitian ini.

DAFTAR PUSTAKA

Arif, B. N. (2005). *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia.* Jakarta: PT Raja Grafindo Persada.

Bakhri, S. (2011). *Pengaruh Aliran-Aliran Falsafat Pemidanaan Dalam Pembentukan Hukum Pidana Nasional.* Jakarta : Cakrawala.

Hamzah, A. (2005). *Aspek-aspek Pidana di Bidang Komputer.* Jakarta: Sinar Grafika.

Kristiawanto. (2021). *Perbandingan Hukum Pidana.* Jakarta: Cakrawala.

Mamudji, S. S. (2009). *Penelitian Hukum Normatif; Suatu Tinjauan Singkat.* Jakarta: Raja Grafindo Persada.

Maramis, F. (2016). *Hukum Pidana Umum dan Tertulis di Indonesia.* Jakarta: Rajawali Pers.

Marzuki, P. M. (2005). *Penelitian Hukum.* Jakarta: Kencana Prenada Media Group.

McGregor, G. H. (1995). *Mastering The Internet.* California: Sybex.

Poerwadarminta, W. (1996). *Kamus Umum Bahasa Indonesia.* Jakarta: Balai Pustaka.

Prodjodikoro, W. (2003). *Tindak Pidana Tertentu di Indonesia.* Jakarta: Refika Aditama.

Prodjohamidjojo, M. (1996). *Memahami Dasar-Dasar Hukum Pidana Indonesia II.* Jakarta: Pradnya Paramita.

Rahardjo, S. (1987). *Masalah Penegakan Hukum.* Bandung: Sinar Baru.

Ramlani Lina S. (2021). *Buku Panduan Penulisan Desertasi dan Tesis.* Jakarta: Universitas Jayabaya.

Saleh, P. R. (2013). *Hukum Pidana Perkembangan dan Pertumbuhannya .* Yogyakarta: Total Media.

Setiawan, D. (2005). *Sistem Keamanan Komputer.* Jakarta: PT Elex Media Komputindo.

suseno, S. (2012). *Yurisdiksi Tindak Pidana.* Bandung: PT Refika Aditama.

Widodo. (2011). *Aspek Hukum Kejahatan Mayantara.* Yogjakarta: Aswindo.