PAMPAS: *Journal Of Criminal Law*
Volume 5 Nomor 2, Tahun 2024
(ISSN 2721-8325)

Pertanggungjawaban Pidana *Hacktivist* dalam Perspektif Hukum Pidana di Indonesia

Puan Maharani, Hafrida, Mohamad Rapik
Fakultas Hukum, Universitas Jambi
Author's Email Correspondence: puanmaharani767@gmail.com

ABSTRAK
Artikel ini bertujuan untuk menganalisis pertanggungjawaban pidana *hacktivist* di Indonesia. Dalam era digital yang semakin maju, hacktivisme telah menjadi fenomena yang signifikan di dunia maya. Pelaku yang melakukan hacktivisme disebut *hacktivist*, ialah individu atau kelompok yang menggunakan teknik peretasan untuk menyuarakan ambisi sosial politik atau menyampaikan pesan ideologi terkait isu-isu yang terjadi di masyarakat. Secara khusus, artikel ini mempermasalahkan bagaimana pertanggungjawaban pidana *hacktivist* di Indonesia dan bagaimana kebijakan hukum dari pertanggungjawaban pidana *hacktivist* di Indonesia ke depannya. Sebagai penelitian yuridis normatif, artikel ini mengacu pada peraturan perundang-undangan yang berlaku. Hasil penelitian ini menunjukkan bahwa pertanggungjawaban pidana *hacktivist* di Indonesia mengalami beberapa hambatan, antara lain tidak diaturnya hacktivisme secara khusus dalam peraturan perundang-undangan dan hambatan dalam penegakan hukum yang mempengaruhi pertanggungjawaban pidana oleh *hacktivist*. Oleh karena itu, diperlukan pembaharuan hukum pidana terhadap peraturan perundang-undangan agar hacktivisme dapat dikenakan sanksi secara khusus serta upaya penanggulangan *cybercrime* yang lebih efektif. Selain itu, diperlukan kerjasama yang erat antara pihak berwenang dan lembaga penegak hukum untuk meningkatkan kemampuan dalam menangani serangan siber dan memastikan pertanggungjawaban pidana yang efektif terhadap *hacktivist*.

Kata Kunci: Pertanggungjawaban Pidana, *Cybercrime*, *Hacktivist*.

ARTICLE HISTORY
Submission: 2024-05-15
Accepted: 2024-06-10
Publish: 2024-06-16

KEYWORDS: *Criminal Liability, Cybercrime, Hacktivist.*

ABSTRACT
This article aims to analyze the criminal liability of hacktivists in Indonesia. In an increasingly advanced digital era, hacktivism has become a significant phenomenon in cyberspace. Hacktivists are individuals or groups who use hacking techniques to voice socio-political ambitions or convey ideological messages related to issues that occur in society. Specifically, this article concerns how the criminal liability of hacktivists in Indonesia and how the legal policy of criminal liability by hacktivists in Indonesia in the future. As normative juridical research, this article refers to the applicable laws and regulations. The results of this study indicate that hacktivists criminal liability in Indonesia experiences several obstacles, including the absence of specific regulation of hacktivism in legislation and obstacles in law enforcement that affect criminal liability by hacktivists. Therefore, it is necessary to reform the criminal law into legislation so that hacktivism can be specifically sanctioned as well as more effective cybercrime

countermeasures. In addition, close cooperation between authorities and law enforcement agencies is needed to improve the ability to deal with cyber attacks and ensure effective criminal liability for hacktivists.

A. PENDAHULUAN

Teknologi informasi dan komunikasi pada era globalisasi memainkan peran penting karena menyajikan suatu dunia yang bebas dari jarak dan waktu. Kehadiran era ini telah memberikan dampak yang signifikan terhadap berbagai lapisan masyarakat, termasuk individu, perusahaan, dan bahkan pemerintah. Sehingga memaksa masyarakat untuk mengadopsi realitas baru yang dikenal dengan dunia maya (*cyberspace*). Perkembangan teknologi informasi dan komunikasi di setiap negara telah mendorong munculnya ancaman-ancaman baru di dunia maya, sehingga sebuah negara harus membangun kapasitas keamanan siber sebagai upaya untuk memberikan keamanan dan keselamatan di dunia maya.[1]

Penggunaan teknologi yang besar jika tidak dimanfaatkan dengan bijak akan melahirkan kejahatan dunia maya (*cybercrime*) yang termasuk perkembangan dari *computer crime*. *Cybercrime* muncul karena revolusi teknologi informasi dan berbeda dengan kejahatan konvensional biasa. Di antara berbagai bentuk *cybercrime* yang ada, muncul satu tren yang dinamakan hacktivisme yang merupakan metode protes digital yang menggunakan peretasan untuk mempromosikan agenda sosial politik. Karatzogianni menyatakan bahwa hal ini merujuk pada ketika individu mengorganisir melalui internet untuk melakukan protes atau ketika mereka menggunakan jaringan untuk menyampaikan pesan politik. Orang yang melakukan perbuatan hacktivisme disebut juga dengan *hacktivist*. *Electronic Frontier Foundation* (EFF) yang berbasis di Amerika Serikat, secara sederhana mendefinisikan *hacktivist* sebagai orang yang menggunakan komputer dan jaringan sebagai alat protes atau aksi.[2]

Para *hacktivist*, termasuk Anonymous, Julian Assange, dan Edward Snowden memiliki pengaruh besar dalam fenomena politik global. *Hacktivist* menargetkan pemerintah, industri besar, perusahaan multinasional, dan individu yang memiliki pengaruh signifikan. Dengan motivasi *hacktivist* dapat berasal dari pandangan politik, suku, etnis, kepercayaan, dan ideologi tertentu dalam cakupan nasional atau global.

Di Indonesia, paradigma peretasan model ini mulai berkembang sebagai respon terhadap isu politik hangat di masyarakat. Salah satunya seperti kehadiran Bjorka yang melabeli dirinya sebagai *hacktivist* untuk bangsa Indonesia. Bjorka membocorkan berbagai informasi rahasia dari pemerintah seperti Komisi Pemilihan Umum, data pribadi registrasi nomor seluler, hingga BUMN seperti Pertamina.[3] Sebelumnya, protes *hacktivist* terjadi terkait mahalnya harga kuota internet dan mengakibatkan situs web milik Telkomsel di *deface* yang menampilkan pesan kritik atas mahalnya tarif kuota internet dari Telkomsel.

---

[1] A Fathan Taufik, Indonesia's Cyber Diplomacy Strategy As A Deterrence Means to Face The Threat in The Indo-Pacific Region. *Journal of Physics: Conference Series* 1721. No. 1. 2021. hlm. 1.

[2] Francesca Farmer, Cybercrime vs Hacktivism: Do We Need A Differentiated Regulatory Approach? Inggris: Universitas Exeter, 2022. hlm. 56.

[3] Rifan Kurnia, The Rise of Hacktivism and Emerging Issues in Data Protection in Indonesia. *ResearchGate*. 2022. hlm. 1.

Hacktivist berbeda dengan jenis peretas lainnya, karena motivasi *hacktivist* didasarkan oleh keinginan terkait perubahan sosial politik, bukan terkait finansial.[4] Hacktivisme dapat terjadi dalam berbagai bentuk, diantaranya perusakan situs web hingga pembobolan dan kebocoran data baik individu, kelompok, atau organisasi dengan agenda atau tujuan tertentu. Perusahaan keamanan siber, Panda *Security*, mendeskripsikan hacktivisme sebagai bentuk aktivisme digital tanpa kekerasan di mana motifnya bukanlah keuntungan finansial pribadi. Sebaliknya, kampanye *hacktivist* bertujuan untuk mencapai keadilan politik, sosial, atau agama yang sejalan dengan tujuan kelompok.[5]

Donalds dan Osei Bryson membuat taksonomi *cybercrime* yang menjelaskan bahwa hacktivisme dapat dilihat sebagai kejahatan siber karena mencakup korban (misalnya pemerintah yang menjadi korban serangan DoS); penyerang (misalnya kelompok *hacktivist* yang melakukan peretasan) yang menggunakan keterampilan teknis mereka untuk melewati sistem keamanan untuk mempromosikan tujuan politik mereka.[6]

Dalam hal ini, *hacktivist* merupakan pelaku kejahatan dunia maya yang melanggar hukum dan merugikan pihak lain. *Hacktivist* yang melakukan perbuatan kriminal harus bertanggung jawab secara hukum atas perbuatannya. Dalam ranah hukum pidana, seseorang melakukan kesalahan dapat dikenakan tanggung jawab atas perbuatannya jika kesalahan tersebut memenuhi unsur-unsur dari pertanggungjawaban pidana. Jika pembuktian kejahatan seseorang menitikberatkan pada perbuatannya maka penentuan seseorang dapat dikatakan bersalah dan secara sah melawan hukum harus dibuktikan untuk memperoleh kepastian hukum.

Indonesia telah memiliki 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. Terdapat pengaturan tentang hacktivisme yang secara tersurat diatur dalam peraturan hukum di Indonesia.

Dari berbagai bentuk hacktivisme yang terjadi di Indonesia dapat dikenakan Pasal UU ITE dan UU PDP yang menyerang data dan sistem elektronik milih orang lain. Namun, jika dikaitkan dengan perbuatan seperti perusakan situs web dapat dikenakan Pasal 30 dan Pasal 32 ayat (1) UU ITE tentang akses ilegal dan perusakan situs web dikaitkan dengan aktivitas memodifikasi situs web tanpa hak. Sementara pembobolan dan kebocoran data dapat dikenakan Pasal 26 ayat (1), Pasal 32 UU ITE, dan Pasal 65 ayat (2) UU PDP.

Namun, penting untuk dicatat bahwa interpretasi dan penerapan pasal-pasal di atas terhadap hacktivisme dapat bervariasi dan memerlukan analisis lebih lanjut untuk memahami hacktivisme. Dalam hal ini, hacktivisme yang tidak diatur secara khusus dalam peraturan di atas menjadikan penafsiran dari hacktivisme dalam undang-undang masih bersifat terbatas, sehingga penegakan hukum tidak dapat ditegakkan jika hukumnya

[4] Pratama Persadha, Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber di Indonesia," *Jurnal Penelitian Ilmu-Ilmu Sosial*. Vol. 21, No. 2. 2020. hlm. 73.

[5] *Francesca* Farmer, *Op. Cit.* hlm. 162.

[6] *Ibid*, hlm. 51.

mengalami kekaburan yang dibuktikan dengan penafsiran yang terbatas dan/atau konsepnya yang tidak jelas. Sehingga, bagaimana dapat suatu aturan ditegakkan secara efektif bagi pelaku tindak pidana jika hukumnya tidak tegas dan jelas.

Dalam konteks hacktivisme, terdapat tantangan dalam mengidentifikasi dan mengevaluasi hacktivisme sebagai tindak pidana yang jelas diatur oleh hukum. Seperti terdapat tantangan dalam menangkap *hacktivist* karena beberapa kegiatan *hacktivist* dianggap sebagai bentuk aktivisme atau protes yang sah, masyarakat percaya bahwa hacktivisme memainkan peran penting dalam masyarakat. Hal ini menunjukkan bahwa sulit untuk menentukan apakah hacktivisme termasuk kegiatan yang legal atau ilegal.[7] Selain itu, kejahatan ini juga tidak mengenal yurisdiksi sehingga menyulitkan penegak hukum untuk mengkoordinasikan dalam upaya menuntut mereka.

Akibat dari hal tersebut, berdampak pada pertanggungjawaban pidana *hacktivist* di Indonesia yang menghadapi berbagai tantangan dan hambatan. Seperti kompleksitas teknis serangan siber dan kemampuan adaptasi *hacktivist* menjadi kendala dalam mengidentifikasi dan menangkap pelaku. Selain itu, ketidakjelasan sistem perumusan norma dalam pertanggungjawaban pidana bagi *hacktivist* menjadi tantangan yang disebabkan kurang optimalnya sarana dan fasilitas penegakan hukum yang belum memadai. Dalam menghadapi tantangan ini, penegak hukum perlu memperbarui dan menyesuaikan kebijakan serta regulasi untuk mengatasi hacktivisme di Indonesia.

Berdasarkan uraian-uraian di atas, penulis ingin mengetahui pertanggungjawaban pidana oleh *hacktivist* di Indonesia, dapat diharapkan bahwa penelitian ini akan memberikan pengetahuan lebih dalam tentang pertanggungjawaban pidana *cybercrime* oleh *hacktivist* di Indonesia. Dari hal tersebut penulis tertarik untuk melakukan penelitian dan menuangkan dalam artikel dengan judul "Pertanggungjawaban Pidana *Hacktivist dalam Perspektif Hukum Pidana* di Indonesia".

B. METODE PENELITIAN

Penulis menggunakan pendekatan khusus yaitu penelitian yuridis normatif yang disesuaikan dengan isu atau permasalahan yang dibahas. Metode penelitian ini berfokus pada analisis terhadap peraturan perundang-undangan, literatur dan bahan referensi lainnya untuk mengembangkan argumen hukum.

C. PEMBAHASAN

1. Pertanggungjawaban pidana *hacktivist* di Indonesia

Modus operandi kejahatan yang terjadi di masyarakat semakin modern seiring dengan kemajuan peradaban. Hal ini sesuai dengan adagium "dimana ada masyarakat disitu ada kejahatan". Di indonesia, terdapat beberapa kasus hacktivisme yang mengikuti beragam isu hangat di masyarakat. Untuk membahas mengenai pertanggungjawaban pidana oleh *hacktivist*, penulis menjabarkan kasus situs web Telkomsel tahun 2017 dan kasus Bjorka tahun 2022.

Kasus situs web Telkomsel di *deface* pada April 2017, para peretas menyuarakan ketidaksenangan terhadap tarif kuota internet Telkomsel yang tinggi dalam aksi demonstrasi. Pesan dari peretas merupakan permintaan kepada Telkomsel untuk mengakhiri tindakan monopoli terselubungnya. Peretas mengubah nama tampilan Telkomsel diubah menjadi "Telkomnyet". Setelah kejadian tersebut, beberapa

[7] Francesca Farmer, *Op. Cit*. hlm. 171.

pengguna internet mengucapkan terima kasih kepada peretas dan mendukung pesan protes yang disampaikan.[8] Pelaku peretasan pada situs web telkomsel melanggar Pasal 30 dan Pasal 32 ayat (1) UU ITE dengan melakukan perbuatan yang dilarang yaitu mengakses sistem elektronik dan melakukan aktivitas tanpa hak mengubah dan menghilangkan informasi elektronik pada web telkomsel dengan ancaman pidana penjara antara 6 tahun hingga 10 tahun.

Sementara sepanjang tahun 2022, Bjorka telah mengunggah banyak data berupa 1,3 miliar register kartu seluler, 105 juta daftar pemilih di KPU, dan 26 juta pengguna Indihome yang Bjorka unggah di situs *Breached Forums* yang aktif sejak Agustus 2022. Bjorka juga membagikan data pribadi milik sejumlah pejabat publik Indonesia melalui grup Telegramnya seperti data milik Menkominfo yang meliputi NIK, nomor Kartu Keluarga, alamat, nomor telepon, nama anggota keluarga, hingga KTP.[9] Perbuatan Bjorka pada kasus ini melanggar Pasal 26 ayat (1), Pasal 32 UU ITE, dan Pasal 65 ayat (2) UU PDP mengatur mengenai perbuatan pembobolan dan kebocoran data pribadi milik orang lain.

Tanggung jawab pidana mengacu pada hukuman bagi seorang atas tindak pidana yang dilakukan dan memenuhi unsur dalam undang-undang. Apabila suatu perbuatan bertentangan dengan hukum, seseorang dianggap bertanggung jawab secara pidana. Dalam konteks hacktivisme, penentuan pertanggungjawaban pidana bagi *hacktivist* bergantung pada pembuktian kesalahan pelaku dan adanya perbuatan yang melanggar hukum. Untuk menentukan apakah suatu perbuatan dapat dijadikan dasar untuk dipidana atau tidak, hal tersebut merujuk asas legalitas dalam Pasal 1 ayat (1) KUHP. Beccaria menyatakan hanya undang-undang yang dapat memutuskan perbuatan apa saja yang dapat dipidana, sanksi apa yang dapat dijatuhkan, dan bagaimana peradilan pidana harus dilaksanakan.[10]

Untuk menentukan apakah hacktivisme merupakan tindak pidana, perlu dianalisis berdasarkan asas legalitas. Sebelum berlakunya UU ITE dan UU PDP, KUHP mengatur penegakan hukum terhadap kejahatan terkait komputer yang secara tidak langsung terkait dengan masalah kejahatan siber. Untuk mengisi kekosongan hukum dalam kejahatan siber, pasal KUHP menafsirkan objek sebagai benda tidak berwujud seperti elektronik dan komputer. Misalnya Pasal 406 KUHP yang membahas *hacking* seperti perusakan terhadap situs web atau program menjadi tidak berfungsi. Pasal 167 ayat (1) KUHP terkait dengan menerobos sistem keamanan komputer milik orang lain. Sementara Pasal 513 KUHP yang mengatur penggunaan data pribadi tanpa persetujuan pemilik sebagai tindakan yang melanggar hukum.

UU ITE dan UU PDP diundangkan sebagai hukum pidana khusus untuk menangani *cybercrime* sesuai dengan asas *lex specialis derogate legi generali*, undang-undang tersebut mengesampingkan ketentuan pasal KUHP yang terkait dengan *cybercrime*, termasuk hacktivisme. KUHP yang ada saat ini tidak cukup untuk menjawab perkembangan teknologi informasi dan kejahatan siber. Oleh karena itu, UU

[8] Pratama Persadha, *Op. Cit.* hlm. 74.

[9] Rifan Kurnia, *Op. Cit.* hlm. 6-7.

[10] Chairul Huda, *"Dari 'Tiada Pidana Tanpa Kesalahan' Menuju Kepada 'Tiada Pertanggungjawaban Pidana Tanpa Kesalahan": Tinjauan Kritis terhadap Teori Pemisahan Tindak Pidana dan Pertanggungjawaban Pidana*. Jakarta: Kencana. 2021. hlm. 20–21.

ITE dan UU PDP hadir untuk membangun kerangka hukum yang lebih spesifik dan komprehensif.

Pengaturan pasal dalam UU ITE dan UU PDP yang berkaitan dengan perusakan situs web hingga pembobolan dan kebocoran data oleh *hacktivist* sebagai berikut:

a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Hacktivist yang melakukan perbuatan perusakan situs web (*website defacements*) yaitu peretas yang mengakses situs web dan mengubah tampilan untuk mempromosikan pesan politik atau sosial dan mengganggu operasi situs web. Peretas juga dapat meninggalkan pesan yang menjelaskan motivasi mereka untuk melakukan serangan. Perbuatan yang mengakses dan memodifikasi situs web tanpa hak melanggar Pasal 30 dan Pasal 32 ayat (1).

Pasal 30 menyatakan:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 32 ayat (1) menyatakan:

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/atau dokumen elektronik milik orang lain atau milik publik.

Sementara *hacktivist* yang melakukan pembobolan dan kebocoran data yaitu mengekspos informasi sensitif dan mempromosikan suatu isu. Hal ini melibatkan akses ke basis data atau sistem dan mencuri informasi rahasia, seperti kata sandi pengguna atau nomor kartu kredit. Informasi tersebut kemudian dibocorkan ke publik atau diposting di internet, dengan tujuan untuk mempermalukan atau merusak reputasi target. Perbuatan ini melanggar Pasal 26 ayat (1) dan Pasal 32.

Pasal 26 ayat (1) menyatakan:

Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan

Pasal 32 menyatakan:

(1) 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/atau dokumen elektronik milik orang lain atau milik publik.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Berdasarkan Pasal 26 ayat (1) dan Pasal 32, pembobolan dan kebocoran data yang dilakukan oleh *hacktivist* dengan cara menggunakan data pribadi yang bersifat rahasia dapat diakses oleh publik.

b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Dewan Perwakilan Rakyat mengesahkan UU PDP tahun 2022 yang menjawab kekhawatiran akan perlindungan data pribadi yang semakin meningkat di Indonesia yang mencakup informasi pribadi dan data pribadi. Hacktivisme yang berkaitan dengan data pribadi diatur dalam Pasal 65 ayat (2). Pasal 65 ayat (2) menyatakan:

> Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.

Dari kasus yang telah dijelaskan di atas terdapat kendala dalam penegakan hukum terkait pertanggungjawaban pidana oleh *hacktivist*. Hal ini berkaitan dengan pasal-pasal pada peraturan di atas belum memberikan penjelasan konkrit mengenai hacktivisme. Sehingga terdapat kesulitan dalam memahami bentuk hacktivisme dan apa itu arti hacktivisme yang jelas diatur dalam undang-undang. Akibatnya terjadi kesulitan bagi penegak hukum dalam penerapan pasal bagi *hacktivist* yang melakukan *cybercrime*.

2. Kebijakan Hukum dari Pertanggungjawaban Pidana *Hacktivist* di Indonesia ke Depannya

Di Indonesia, keberadaan *hacktivist* telah menimbulkan pertanyaan tentang bagaimana hukum dapat menangani kegiatan mereka. Oleh karena itu, kebijakan hukum dalam pertanggungjawaban pidana terhadap *hacktivist* perlu diperhatikan dan dikembangkan di masa depan. Saat ini, Indonesia masih belum memiliki peraturan yang mengatur hacktivisme secara khusus. Meskipun demikian dalam UU ITE dan UU PDP mengandung sejumlah pasal yang mengatur hacktivisme secara tidak langsung yang digunakan sebagai payung hukum untuk hacktivisme meskipun tidak dituangkan secara tersurat dalam rumusan pasal-pasalnya.

Terdapat permasalahan dalam menangani hacktivisme, permasalahan yang muncul meliputi kekaburan norma dan kurangnya pemahaman tentang *cybercrime*. Beberapa masyarakat menganggap *hacktivist* sebagai pahlawan yang berjuang untuk keadilan sosial atau kebebasan informasi, sementara yang lain menganggap mereka sebagai penjahat yang merusak tatanan sosial dan melanggar hukum.

Dalam melakukan perbuatannya, *hacktivist* memiliki 3 hal yang dapat mendukungnya. Pertama, partisipan dalam hacktivisme tidak membutuhkan dana yang besar, hal pokok yang diperlukan adalah komputer dan internet. Kedua, *hacktivist* memiliki anonimitas di internet yang menjadi kunci untuk *hacktivist* tidak diketahui dalam waktu yang lama, karena prosesnya bersifat virtual dan tidak bertemu langsung. Ketiga, *hacktivist* memiliki kerentanan diserang lebih rendah, hal ini disebabkan karena *hacktivist* cenderung membatasi teknologi yang umum dipakai awam.[11]

Sorell berpendapat bahwa masalah utama hacktivisme adalah karena anonimitasnya. *Hacktivist* cenderung tidak memiliki kewarganegaraan, sulit dipahami, terkadang tidak memiliki hukum, dan hampir selalu anonim. Mereka juga tidak dapat dipertanggungjawabkan di negara-negara yang melindungi hak kebebasan berbicara dan hak privasi. Karena anonimitas, *hacktivist* tidak terlalu terhambat dalam mengekspresikan ide-ide yang penuh kebencian atau kekerasan dibandingkan dengan mereka yang mengekspresikannya secara terbuka.[12]

Permasalahan pemahaman masyarakat tentang *cybercrime* dan serangan siber oleh *hacktivist* masih terbatas. Hal ini mempersulit upaya untuk mendeteksi, melaporkan, dan menangani kejahatan siber dengan efektif. Pendidikan dan kesadaran publik tentang *cybercrime* perlu ditingkatkan agar masyarakat dapat berperan aktif dalam melindungi diri dan melaporkan kegiatan yang mencurigakan terkait sistem informasi dan komunikasi.

Berdasarkan permasalahan di atas berpotensi meningkatkan praktik hacktivisme mengarah pada seruan untuk kepastian hukum yang lebih besar dan rasa keadilan terkait pertanggungjawaban pidana. Mempertanggungjawabkan seseorang membutuhkan keyakinan yang kuat bahwa sudah pada tempatnya untuk meminta tanggung jawab atas tindak pidana yang telah diperbuat. Pertanggungjawaban pidana pada dasarnya mengacu pada keadaan bertanggung jawab atas tindak pidana. Pertanggungjawaban pidana mensyaratkan adanya hubungan terkait keadaan pembuat dan perbuatan serta hukuman yang seharusnya dijatuhkan.[13]

Diperlukan pemahaman yang khusus mengenai hacktivisme, kepastian pemahaman tentang aktivitas kriminal yang sedang berkembang sangat penting untuk mengembangkan strategi komprehensif yang bertujuan untuk mengurangi kemampuan *hacktivist* melakukan serangan ke jaringan atau komputer sebagai platform aktivisme digital. Situasi ini berkaitan dengan bagaimana kebijakan hukum pidana indonesia terkait pertanggungjawaban pidana *hacktivist*. Kebijakan hukum pidana menjadi suatu usaha untuk mengembangkan legislasi pidana yang selaras dengan kondisi dan situasi saat ini serta di masa depan. Upaya ini diharapkan menjadi langkah efektif untuk mengatasi hacktivisme.

Kebijakan hukum pidana ke depan perlu memperhatikan perkembangan serangan siber dengan berbagai motif khususnya motif sosial, politik, dan ideologi. Seperti kasus *hacktivist* yang menyerang pemerintah dan lembaga penting yang dilakukan Bjorka. Kebijakan hukum pidana terhadap pertanggungjawaban pidana

[11] Muhammad Fikry Anshori, Hacktivist pada Pergerakan Sosial Transnasional: Kampanye Anonymous Melawan Jaringan Teroris Transnasional 2015-2016. *Andalas Journal of International Studies (AJIS)*. Vol. 8, No. 2. 2019. hlm. 171-172.

[12] Francesca Farmer, *Op. Cit*. hlm. 61.

[13] Chairul Huda, *Op. Cit.* hlm. 65–66.

hacktivist dengan menggunakan fasilitas teknologi harus diseimbangkan dengan pembenahan dan pembangunan secara menyeluruh terhadap sistem hukum pidana. Kebijakan hukum pidana mengambil peran penting dalam penegakan hukum dan kebijakan sosial yang mempengaruhi sistem peradilan pidana. Adanya suatu korelasi terkait kebijakan penegakan hukum dan sistem peradilan pidana, khususnya subsistem sistem peradilan pidana yang bertanggung jawab atas penanggulangan kejahatan.[14]

Mewujudkan penegakan hukum yang lebih komprehensif dan menghasilkan kepastian hukum, diperlukannya pembaharuan hukum pidana (*penal reform*) terhadap hacktivisme di Indonesia menjadi hal yang penting untuk dimasukan pengaturannya ke dalam undang-undang. Upaya pembaharuan hukum pidana ini terkait dengan pengembangan regulasi tentang hacktivisme. Pembaharuan hukum pidana adalah elemen krusial kebijakan hukum pidana yang bertujuan menciptakan peraturan yang sangat efektif dan selaras dengan kondisi masyarakat dan tujuan negara. Hal ini membutuhkan pendekatan kebijakan dan dilakukan secara efektif untuk mencapai hasil yang diinginkan.

Hingga saat ini, terbatasnya pertanggungjawaban yang mengatur hacktivisme dapat diamati dan dirasakan sebagai ketidakseimbangan dan ketidaktegasan pertanggungjawaban pidana *hacktivist* di Indonesia. Pembaharuan hukum pidana terkait hacktivisme dapat dilakukan penyesuaian terhadap jenis kejahatan yang diatur, peningkatan atau penurunan sanksi yang diberikan, pengenalan kejahatan baru yang berkaitan dengan perkembangan teknologi atau masalah sosial, atau perubahan dalam proses peradilan pidana. Tujuannya adalah untuk memastikan bahwa hukum pidana tetap relevan, efektif, dan responsif terhadap perkembangan sosial, teknologi, dan kebutuhan masyarakat dalam menangani kejahatan, terutama kejahatan yang terjadi pada dunia maya.

Sampai saat ini, UU ITE dan UU PDP telah mengatur hukuman bagi pelaku peretasan, namun perlu diperluas dan disempurnakan dengan pembaharuan hukum pidana untuk mengakomodasi perkembangan teknologi dan metode kejahatan baru yang belum diatur dengan jelas dalam undang-undang. Dengan adanya pembaharuan hukum pidana yang komprehensif akan membantu menciptakan kerangka hukum yang lebih jelas dan dapat diandalkan dalam menangani kasus-kasus kejahatan siber.

Selain itu, penting untuk memperkuat kerjasama internasional, pemerintah dapat memperkuat kerjasama dalam penanggulangan *cybercrime* dengan negara-negara lain. Indonesia dapat memanfaatkan pengalaman dan keahlian bersama untuk melawan hacktivisme dan kejahatan siber lainnya yang melintasi batas negara. Kerjasama ini dapat meliputi pertukaran informasi, harmonisasi hukum, koordinasi penegakan hukum lintas negara, dan diplomasi siber (*cyber diplomacy*). Langkah-langkah kebijakan masa depan juga dapat mencakup pengembangan tim ahli di bidang keamanan siber dan pemahaman masyarakat terhadap *cybercrime*.

Penjelasan di atas berkaitan dengan salah satu upaya penanggulangan kejahatan melalui hukum pidana yang merupakan usaha penegakan hukum. Politik hukum pidana merupakan merupakan salah satu komponen dari kebijakan penegakan hukum, hal tersebut menjadi upaya mengatasi masalah sosial termasuk dalam bidang

[14] Muhamad Hasan Rumlus dan Aldilla Yulia Wiellys Sutikno, Kebijakan Reformulasi Tindak Pidana Penipuan Dalam Transaksi Elektronik (Reformulation Policy of Fraud in Electronic Transactions). *Jurnal Ilmu Hukum: Equality Before The Law*. Vol. 1, No. 2. 2022. hlm. 10–11.

kebijakan penegakan hukum. Kebijakan penegakan hukum bertujuan untuk mencapai kesejahteraan masyarakat, tercakup dalam kebijakan sosial yang terdiri dari semua upaya rasional untuk mencapai kesejahteraan masyarakat.

Kebijakan hukum pidana terhadap pertanggungjawaban pidana *hacktivist* sangat mendesak untuk dilakukan, hal ini dilakukan agar tercapai kepastian hukum. Pembaharuan hukum pertanggungjawaban pidana *hacktivist* di Indonesia bertujuan untuk mengatasi tantangan yang terkait dengan kejahatan siber oleh *hacktivist*. Dengan pembaharuan hukum pidana, diharapkan penegakan hukum terhadap *hacktivist* di Indonesia dapat lebih efektif dalam menghadapi perkembangan kejahatan siber yang semakin kompleks dan melindungi masyarakat dari ancaman *cybercrime*.

Berdasarkan uraian di atas, kebijakan hukum mengenai *hacktivist* di Indonesia perlu dilakukan dengan pendekatan penal dan non penal. Penal, berbentuk pembaharuan kebijakan hukum pidana untuk mengefektifkan hukum positif yang berkaitan dengan hacktivisme. Non penal, berbentuk upaya pencegahan terjadinya hacktivisme. Kebijakan hukum pidana mengenai pertanggungjawaban pidana oleh *hacktivist* perlu untuk diperbaharui, hal ini terjadi karena belum adanya aturan hukum secara khusus tentang hacktivisme. Kebijakan hukum secara penal dan non penal dilakukan agar memaksimalkan penegakan hukum dalam pertanggungjawaban pidana kepada *hacktivist* ke depannya.

D. SIMPULAN

Pertanggungjawaban pidana *hacktivist* di Indonesia bergantung pada pembuktian kesalahan pelaku dan adanya perbuatan yang melanggar hukum. Pengaturan pertanggungjawaban pidana *hacktivist* di Indonesia diatur dalam UU ITE dan UU PDP. Aturan tersebut mengandung sejumlah pasal yang mengatur hacktivisme secara tidak langsung yang digunakan sebagai payung hukum untuk hacktivisme meskipun tidak dituangkan secara khusus dalam rumusan pasal-pasalnya.

Kebijakan hukum dari pertanggungjawaban pidana *hacktivist* di Indonesia ke depannya perlu dilakukannya pembaharuan hukum pidana terkait hacktivisme yang menjadi hal penting untuk dimasukan pengaturannya ke dalam undang-undang dengan tujuan tercapai kepastian hukum. Hacktivisme yang belum secara eksplisit diatur dalam undang-undang dengan dihubungkan dengan pembaharuan hukum pidana akan terbentuknya peraturan tentang hacktivisme yang akan diancam dengan suatu sanksi yang berupa pidana secara khusus.

DAFTAR PUSTAKA

Dokumen Hukum

Kitab Undang-Undang Hukum Pidana. Tahun 1946.

Republik Indonesia, Undang-Undang Tentang Informasi Dan Transaksi Elektronik. UU Nomor 11 Tahun 2008. LNRI Tahun 2008 Nomor 58, TLNRI Nomor 4843.

Republik Indonesia, Undang-Undang Tentang Perlindungan Data Pribadi. UU Nomor 27 Tahun 2022. LNRI Tahun 2022 Nomor 196, TLNRI Nomor 6820.

Buku

Huda, Chairul, "Dari 'Tiada Pidana Tanpa Kesalahan' Menuju Kepada 'Tiada

Pertanggungjawaban Pidana Tanpa Kesalahan": Tinjauan Kritis terhadap Teori Pemisahan Tindak Pidana dan Pertanggungjawaban Pidana. Jakarta: Kencana, 2021.

Jurnal/ Majalah Ilmiah

Anshori, Muhammad Fikry, "Hacktivist Pada Pergerakan Sosial Transnasional: Kampanye Anonymous Melawan Jaringan Teroris Transnasional 2015-2016", Andalas Journal of International Studies (AJIS), Vol. 8, No. 2 (2019).

Fathan Taufik, A, "Indonesia's Cyber Diplomacy Strategy As A Deterrence Means To Face The Threat in The Indo-Pacific Region", Journal of Physics: Conference Series 1721, No. 1 (2021).

Kurnia, Rifan, "The Rise of Hacktivism and Emerging Issues in Data Protection in Indonesia", ResearchGate, (2022).

Persadha, Pratama, "Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber di Indonesia", JURNAL SOSIAL Jurnal Penelitian Ilmu-Ilmu Sosial, Vol. 21, No. 2 (2020).

Rumlus, Muhamad Hasan, dan Aldilla Yulia Wiellys Sutikno, "Kebijakan Reformulasi Tindak Pidana Penipuan Dalam Transaksi Elektronik (Reformulation Policy Of Fraud In Electronic Transactions) ", Jurnal Ilmu Hukum: Equality Before The Law, Vol. 1, No. 2 (2022).

Tesis

Farmer, Francesca, Cybercrime vs Hacktivism: Do We Need A Differentiated Regulatory Approach? Tesis. Inggris: Universitas Exeter, 2022.