Vol. 9, No. 1, 2024, pp. 10-16
DOI: https://doi.org/10.29210/30033931000

Contents lists available at Journal IICET

JRTI (Jurnal Riset Tindakan Indonesia)
ISSN: 2502-079X (Print) ISSN: 2503-1619 (Electronic)

Journal homepage: https://jurnal.iicet.org/index.php/jrti

Pengaturan hukum *concursus* terhadap pelaku tindak pidana *cyber crime*

Muhammad Aulia Nasution*), Sahuri Lasmadi, Erwin Erwin
Universitas Jambi, Indonesia

Article Info

Article history:

Received Feb 19th, 2024
Revised Mar 28th, 2024
Accepted Apr 17th, 2024

Keyword:

Concursus
Cyber crime
Hukum pidana

ABSTRACT

Penanganan kasus tindak pidana *cyber crime* dapat melibatkan lebih dari satu yurisdiksi atau penuntutan oleh lebih dari satu negara. Tujuan dari penelitian ini adalah untuk menganalisis pengaturan pemidanaan terhadap *cyber crime* dalam hal terjadinya *concursus* tindak pidana. Lebih lanjut penelitian ini bertujuan untuk menganalisis tentang kebijakan hukum pidana terkait perbarengan tindak pidana (*consursus*) dalam kasus *cyber crime* dimasa mendatang. Metode penelitian yang digunakan adalah metode penelitian hukum, yaitu metode yuridis normative. Hasil penelitian menunjukkan bahwa: 1) Pengaturan *concursus* dalam tindak pidana *cyber crime hacker* seharusnya menggunakan konsep *concursus*, baik concursus realis maupun *concursus idealis* karena *cyber crime* dalam melakukan aksinya terdapat perbarengan tindak pidana supaya tercipta keadilan, kepastian, dan kemanfaatan hukum; 2) Formulasi kebijakan hukum pidana dalam tindak pidana cyber crime kedepannya harus ada reformasi hukum dalam bidang *cyber crime* sehingga para pelaku *cyber crime* mendapatkan hukuman yang setimpal atas perbuatannya. Penelitin ini diharapkan dapat dijadikan sebagai acuan kepada aparat penegak hukum dan pemerintah dalam mengemban tugas. Hasil dari penelitian juga dapat dijadikan sebagai landasan dalam melakukan kerja sama, melakukan revisi atau perubahan atas undang-undang *cyber crime* dengan memasukkan prosedur penganti pidana penjara berupa pidana kerja sosial atau pidana pengawasan sebagai pidana tambahan alternatif.

Corresponding Author:

Muhammad Aulia Nasution,
Universitas Jambi
Email: aulianasution272@gmail.com

Pendahuluan

Tindak pidana yang ditimbulkan cenderung semakin meningkat dan semakin kompleks seiring kemajuan masyarakat. Seorang terdakwa yang melakukan dua atau lebih delik secara bersamaan atau terpisah merupakan salah satu kompleksitas tindak pidana modern (S. Muladi, Diah Sulistyani, & SH, 2021). Kasus delik yang dilakukan oleh seorang terdakwa lebih dari satu kali dan belum ada keputusan hakim di antaranya disebut perbarengan (*concursus*) (Insani, 2022). Perbarengan (*concursus*) yang disebutkan di atas terbagi menjadi tiga bagian: pertama, *concursus idealis*; kedua, *concursus continuum*; dan ketiga, *concursus* realis (Azra, 2022; Tarmizi, 2022).

Pengertian perbarengan (*concursus*) di dalam KUHP belum dijelaskan secara langsung di dalam pasal-pasal tetapi unsur-unsur dari perbarengan ada dalam pasal KUHP (Ator, 2021). Unsur-unsur perbarengan

(*concursus*) yang dibagi atas tiga bagian yaitu pertama; *concursus idealis*, terdapat dalam Pasal 63 KUHP yang mengatakan bahwa suatu perbuatan masuk dalam lebih dari satu aturan pidana, kedua; perbuatan berlanjut, terdapat dalam Pasal 64 KUHP yang mengatakan bahwa apabila seseorang melakukan beberapa perbuatan tersebut masing-masing merupakan kejahatan atau pelanggaran antara perbuatan-perbuatan itu ada hubungan sedemikian rupa sehingga harus dipandang sebagai satu perbuatan berlanjut, sedangkan yang terakhir adalah *concursus realis* terdapat dalam Pasal 65 KUHP yang mengatakan apabila seseorang melakukan perbuatan masing-masing perbuatan itu berdiri sendiri sebagai suatu delik (kejahatan/pelanggaran).

Kasus perbarengan (*concursus*) seperti yang dijelaskan di atas merupakan tantangan bagi penegak hukum. Penegak hukum seperti polisi, jaksa dan hakim merupakan tiga institusi yang diberikan kewenangan menangani kasus-kasus kejahatan sesuai dengan pembagian tugas atau fungsi menurut peraturan perundang-undangan. Tantangan masing-masing institusi tersebut berbeda-beda, polisi mempunyai peran mengungkap kejahatan dan menangkap pelakunya (Sitepu, Lubis, & Sahlepi, 2023). Polisi sebagai penyidik dalam melakukan penyidikan kepada tersangka sebuah kejahatan seringkali melakukan kesalahan-kesalahan yang sangat ekstrim seperti pengungkapan kasus-kasus terkait sehingga ada kasus yang terpisah (*splitz*) bahkan yang lebih ironis kesalahan penyidik adalah salah tangkap dan kriminalisasi kepada orang yang di duga melakukan kejahatan (Prakasa & Astoni, 2022). Berbeda halnya dengan peran jaksa sebagi penuntut umum, jaksa harus mampu membuktikan delik yang dilanggar oleh pelaku kejahatan dipersidangan hal ini merupakan kesulitan tersendiri bagi jaksa penuntut umum.

Salah satu kasus perbarengan (*concursus*) yang dapat diuji objektivitas hakim dalam menjatuhkan putusan yaitu kasus *cyber crimer hacker* pernah terjadi di Sleman, Daerah Istimewa Yogyakarta. "Kasus tersebut melibatkan hacker berisinial BBA (21) yang ditangkap karena meretas server sebuah perusahaan di *San Antonio, Texas, Amerika Serikat"* (Kusuma & Khairina, 2019). Menurut Kasubdit Direktorat Tindak Pidana Siber Bareskrim Polri, Kombes Rickynaldo Chairul nenyampaikan, pelaku melakukan tindak pidana hacking dengan modus ransomware. Dia ditangkap pada 18 Oktober 2019 di Yogyakarta. Tersangka ini menyebarkan atau mengirimkan email ke korban, berisi link atau tautan, di mana ketika korban mengklik link itu, akan menyebabkan server komputer mati. Setelah server komputer sasaranya mati, pelaku kemudian meminta uang tebusan dalam bentuk mata uang *crypto currency bitcoin* sebagai syarat untuk mengembalikan fungsi sistem. Dalam beraksi, BBA bisa memeras hingga 300 *bitcoin*. satu *btcoin* itu kalau ditukar nilainya sekitar Rp 150 juta.

Dalam aksinya, dia mengirimkan tautan email http://ddiam.com/shipping200037315.pdf.exe ke salah satu satu karyawan di perusahaan tersebut. Link tersebut mengarahkan pengguna ke link lain berisikan *cryptolocker*. BBA juga diketahui melakukan tindak pidana lain berupa carding dengan modus membelanjakan kartu kredit orang lain dan memperjual belikan data kartu kredit orang lain. Atas perbuatannya itu, BBA dikenakan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (1) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Kusuma & Khairina, 2019).

Pelaku berhasil ditangkap oleh Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian Republik Indonesia di kediamannya Sleman, Yogyakarta pada Jumat 18 Oktober 2019. Upaya penanganan *cyber crime* dalam klasifikasi hacker dibutuhkan keseriusan seluruh pihak mengingat teknologi informasi telah dijadikan sarana berbudaya komunikasi. Keberadaan undang-undang yang mengatur *cyber crime* terutama dalam klasifikasi *hacker* diperlukan, akan tetapi jika pelaksanaanya tidak memiliki kemampuan dan keahlian dalam bidang tersebut dan masyarakat terus menjadi sasaran tujuan pembentukan undang-undang tersebut tidak akan tercapai.

Menurut ketentuan Pasal 30 dan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik milik orang lain dengan cara apapun untuk memperoleh informasi elektronik dan atau dokumen elektronik dikenakan sanksi pidana penjara antara 6 (enam) sampai 8 (delapan) tahun dan atau denda sekitar Rp 1.000.000.000,- (satu miliar rupiah) sampai dengan Rp 2.000.000.000,- (dua miliar rupiah). Meskipun pembentuk Undang-Undang telah merumuskan kententuan pidana seperti dalam ketentuan peraturan diatas, namun pada kenyataannya penegakkan hukum pada cyber crime hacker ini di rasa masih sangat kurang. Hal ini di karenakan dalam pemberian sanksi terhadap pelaku tindak pidana *cyber crime hacker* hanya 6 sampai 8 tahun penjara dan/atau denda sekitar Rp 1.000.000.000,- (satu miliar rupiah) sampai dengan Rp 2.000.000.000,- (dua miliar rupiah). seharusnya dalam kasus *cyber crime hacker* ini kita bisa menggunakan konsep *concursus,* baik *concursus idealis, concursus realis*, dan perbarengan berlanjut dalam menindak pelaku tindak pidana *cyber crime* (Keintjem, 2021; Prodjodikoro, 2008).

Berdasarkan uraian-uraian di atas maka dapat dirumuskan tujuan penelitian adalah untuk menganalisis lebih lanjut mengenai pengaturan pemidanaan terhadp *cyber crime* dengan menggunakan konsep *concursus* dan bagaimana kebijakan hukum pidana terkait *concursus* dalam tindak pidana *cyber crime.*

Metode

Metode penelitian yang digunakan adalah metode hukum normatif dengan tipe *yuridis normative* (Nurhayati, Ifrani, & Said, 2021). Metode penelitian ini dilakukan dengan mempelajari, melihat dan menelaah mengenai beberapa hal yang bersifat teoritis yang menyangkut asas-asas hukum, konsepsi, doktrin-doktrin hukum, peraturan hukum dan sistem hukum yang berkenaan dengan permasalahan penelitian ini (Johan, 2016; Marzuki, 2013). Metode ini melibatkan pemeriksaan berbagai peraturan, prinsip, keputusan pengadilan, doktrin, dan instrumen hukum lainnya yang berkaitan dengan topik yang diteliti penelitian.

Hasil dan Pembahasan

Pengaturan Mengenai Perbarengan Tindak Pidana (*Concursus*) Terhadap *Cyber Crime Hacker* Dalam Hukum Pidana Indonesia

Pengaturan hukum terhadap *cyber crime* dalam bentuk *cyber crime hacker* sebelumnya diaturan di dalam Pasal 362 KUHP tentang pancurian sebagaimana yang diketahui bahwa *cyber hacker* secara umum merupakan tindakan pencurian. Pencurian yang dirumuskan di dalam Pasal 362 KUHP adalah (Saputra Gulo, Lasmadi, & Nabawi, 2020; Sari, 2021):

"Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian**,** dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak Rp900 ribu." Beberapa unsur-unsur yang terdapat didalam Pasal 362 KUHP tersebut, yaitu (Handoko, 2018): barangsiapa, mengambil suatu barang, yang seluruhnya atau sebagaian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum

Berdasarkan unsur-unsur yang telah diuraikan dalam Pasal 362 KUHP tersebut, maka dapat disimpulkan bahwa barangsiapa adalah subjek maksudnya ialah pelaku yang melakukan tindak pidana pencurian. Ada maksud untuk mengambil itu hanyalah apabila barang tersebut diambil oleh orang yang tidak berhak terhadap barang tersebut. Unsur selanjutnya Yang diambil harus sesuatu barang, Kita ketahui bersama bahwa sifat tindak pidana pencurian ialah merugikan kekayan si korban, maka barang yang diambil haruslah berharga. Barang yang diambil harus seluruhnya atau sebagian kepunyaan orang lain, maksudnya kepunyaan orang lain dalam hal ini dimaksudkan bahwa barang yang diambil itu haruslah kepunyaan orang lain atau selain kepunyaan orang yang mengambil tersebut. Pengambilan itu harus dilakukan dengan maksud untuk memiliki barang itu dengan melawan hukum, Dalam hal ini dimaksudkan bahwa timbulnya timbulnya perbuatan itu haruslah berdasarkan adanya keinginan dari si pelaku untuk memiliki barang tersebut dengan cara melawan hukum, dimana letak perbuatan melawan hukum dalam hal ini adalah memiliki barang orang dengan cara mencuri atau mengambil barang orang lain tanpa sepengetahuan pemiliknya. Menurut Wirjono, delik yang paling tepat untuk orang yang mengutakatik komputer untuk mendapatkan suatu barang yang bukan miliknya ialah Pasal 362 karena meliputi hak. Tetapi, tidak memenuhi unsur mengenai informasi elektronik dan/atau dokumen elektronik salah, oleh karena itu Pasal 362 sebenarnya tidak tepat untuk dikenakan terhadap *cyber crime* dalam bentuk *hacker* (Prodjodikoro, 2008).

Disahkannya dan diberlakukannya Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang telah berlaku sampai saat ini. Kita mengenal dan menganut asas "*Lex Specialis Derogat Legi Generali*". Berdasarkan asas *lex specialis derogat legi generali*, berarti aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturanaturan hukum yang umum. Dapat disimpulkan bahwa yang berlaku saat ini untuk mengatur tentang bagaimana pengaturan hukum *cyber crime* dalam bentuk *hacker* tersebut saat ini diatur oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik karena Undang-Undang ini bersifat khusus. Pada saat ini perbuatan hacker tersebut diatur pada Pasal 33 jo Pasal 49 yang dirumuskan sebagai berikut (Undang-Undang, 2016):

> Pasal 33 "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

Pasal 49 "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)."

Adapun unsur yang tertuang pada Pasal 33 tersebut di atas, sebagai berikut: setiap orang, mempunyai kesengajaan serta tanpa hak dengan cara melawan hukum, melakukan tindakan apapun yang berakibat terganggunya sistem elektronik, yang mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya (Undang-Undang, 2016).

Perbuatan *hacker* ini juga tidak hanya membuat terganggunya sistem elektronik, namun juga perbuatan *hacker* ini melakukan sebuah tindakan merusak, menghilangkan, memindahkan, menyembunyikan pada informasi elektronik dan/atau dokumen menyebabkan komputer orang tersebut mengalami mati oleh pelaku *cyber crime* dalam bentuk hacker tersebut. Oleh sebab itu, perbuatan hacker dapat dikenakan Pasal 32 ayat (1) jo Pasal 48 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah melakukan tindakan merusak. Pasal 32 ayat (1) jo Pasal 48 ayat (1) dirumuskan sebagai berikut:

Pasal 32 ayat (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."

Pasal 48 ayat (1) "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah)."

Selain menggangu dan merusak sistem informasi elektronik milik orang lain perbuatan hacker juga melakukan pemerasan dan pengancaman pada korban untuk mengembalikan komputer seperti semula sehingga korban merasa dirugikan oleh pelaku hacker. Maka dari itu perbuatan hacker ini dapat dikenakan Pasal 27 ayat (4) jo Pasal 45 ayat (4) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah malakukan tindakan pemerasan. Pasal 27 ayat (4) jo Pasal 45 ayat (1) di rumuskan sebagai berikut:

Pasal 27 ayat (4). "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman."

Pasal 45 ayat (1) "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Berdasarkan uraian unsur-unsur tersebut di atas, jika dikaitkan dengan kasus hacker yang pernah terjadi yang dilakukan oleh seorang berinisial BBA (21) yang ditangkap karena meretas server sebuah perusahaan di *San Antonio, Texas, Amerika Serikat.* pelaku melakukan tindak pidana hacking dengan modus ransomware. Dia ditangkap pada 18 Oktober 2019 di Yogyakarta. Tersangka ini menyebarkan atau mengirimkan email ke korban, berisi link atau tautan, di mana ketika korban mengklik link itu, akan menyebabkan server komputer mati. Setelah server komputer sasaranya mati, pelaku kemudian meminta uang tebusan dalam bentuk mata uang *crypto currency bitcoin* sebagai syarat untuk mengembalikan fungsi sistem. Dalam beraksi, BBA bisa memeras hingga 300 bitcoin. satu btcoin itu kalau ditukar nilainya sekitar Rp 150 juta.

Dalam aksinya, dia mengirimkan tautan email http://ddiam.com/shipping200037315.pdf.exe ke salah satu satu karyawan di perusahaan tersebut. Link tersebut mengarahkan pengguna ke link lain berisikan *cryptolocker*. BBA juga diketahui melakukan tindak pidana lain berupa carding dengan modus membelanjakan kartu kredit orang lain dan memperjualbelikan data kartu kredit orang lain.

Berdasarkan kasus diatas, BBA dapat dikenakan dengan Pasal 33 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena BBA memenuhi unsur-unsur didalam Pasal 33 tersebut dengan mengirimkan link atau tautan yang dapat membuat komputer menjadi terganggu sistemnya.

Apabilah korban mengklik link itu akan menyebabkan server komputer mati, maka BBA dapat dikenakan Pasal 32 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah memenuhi unsur-unsur didalam Pasal 32 ayat (1) karena dengan sengaja dan tanpa hak menyebabkan komputer seseorang mati.

Pada waktu komputer korban mengalami server mati BBA melakukan tindakan pemerasan dengan cara meminta uang *crypto currency bitcoin* sebagai syarat untuk mengembalikan fungsi sistem, oleh itu BBA dapat dikenakan Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah memenuhi unsur-unsur didalam Pasal 27 ayat (4) karena dengan sengaja dan tanpa hak melakukan pemerasan dan pengacaman.

Pidana yang dijatuhkan terhadap *cyber crime* dalam bentuk hacker seharusnya adalah dikenakan Pasal yang berlapis yaitu Pasal 33 jo Pasal 49, Pasal 32 ayat (1) jo Pasal 48 ayat (1) atau Pasal 27 ayat (4) jo Pasal 45 ayat (1) dan tidak boleh lebih dari maksimum pidana yang terberat ditambah sepertiga, sistem ini dinamakan sistem kumulasi diperlunak (Prasetyo, 2011). Hal ini dinamakan dengan istilah "*Concursus Realis*". *Concursus Realis* terjadi apabila seseorang melakukan beberapa perbuatan, dan masing-masing perbuatan itu berdiri sendiri sebagai suatu tindak pidana dan tindak pidana yang dilakukan tersebut tidak perlu sejenis bahkan tidak perlu berhubungan satu dengan yang lainnya (Prasetyo, 2011). Seperti halnya dengan *cyber crime* dalam bentuk hacker melakukan perbuatan melawan hukum yang melanggar Pasal 33 karena telah membuat terganggunya sistem komputer, namun juga melanggar Pasal 32 ayat (1) dengan mengakibatkan server komputer mati, serta melanggar Pasal 27 ayat (4) dengan melakukan pemerasan dan pengacamana.Berdasarkan uraian di atas, maka didalam Pasal 27 Ayat (4) jo Pasal 45 Ayat (1) dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah), Pasal 32 ayat (1) jo Pasal 48 ayat (1) dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah), dan Pasal 33 jo Pasal 49 dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah) dapat ditentukan bahwa pidana yang terberat ada di Pasal 33 jo Pasal 49 yaitu dengan pidana penjara paling lama 10 tahun dan pidana denda paling banyak Rp 10.000.000.000,00, lalu pidana terberat tersebut ditambahkan sepertiga dari masing-masing pidana terberat. Pertama, pidana penjara 10 tahun + (1/3 x 10) = 13 Tahun. Kedua, pidana denda Rp 10.000.000.000,00 + (1/3 x 10.000.000.000) = Rp 13.000.000.000,00 (tiga belas miliar rupiah). Jadi, jika dijumlahkan pidana penjara 3 tahun + 10 tahun = 13 tahun maka dari itu seharusnya pidana penjara yang akan dijatuhkan paling lama adalah 13 tahun. Dan pidana denda jika dijumlahkan Rp 3.000.000.000,00 + 10.000.000.000,00 = 13.000.000.000,00 (tiga belas miliar rupiah) maka penjatuhan pidana denda tersebut diperbolehkan karena tidak melebihi maksimum pidana denda terberat ditambah sepertiga. Berdasarkan penjabaran tersebut di atas dapat diambil kesimpulan bahwa pidana yang akan dijatuhkan kepada pelaku hacker yang telah melanggar Pasal 33 jo Pasal 49, Pasal 32 ayat (1) jo Pasal 48 ayat (1) dan Pasal 27 ayat (4) jo Pasal 45 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik seharusnya adalah pidana penjara paling lama 13 (tiga belas) tahun dan/atau pidana denda paling banyak Rp 13.000.000.000,00 (tiga belas miliar rupiah).

Sedangkan kalau menggunakan *Concursus Idealis* dalam penegakan *cyber crime hacker* ini kita bisa melihat adanya unsur teror dan pengancaman yang itu termasuk dalam Undang-Undang Nomor 5 Tahun 2018 Tentang Pemberantasan Tindak Pidana Terorisme. Dalam Pasal 1 ayat (2) Undang-Undang Nomor 5 Tahun 2018 Tentang Pemberantasan Tindak Pidana Terorisme disebutkan "Terorisme adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, Iingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan."

Menurut Ketentuan Pasal 1 dan Pasal 6 Undang-Undang Nomor 5 Tahun 2018 Tentang Pemberantasan Tindak Pidana Terorisme (P. R. Indonesia, 1981; Undang-Undang, 2016), Setiap Orang yang dengan sengaja menggunakan Kekerasan atau Ancaman Kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas, menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap Objek Vital yang Strategis, lingkungan hidup atau Fasilitas Publik atau fasilitas internasional dipidana dengan pidana penjara paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun, pidana penjara seumur hidup, atau pidana mati.

Kalau dilihat dari *concursus idealis* bisa saja penegakan hukum *cyber crime hacker* ini menggunakan Undang-Undang Nomor 5 Tahun 2018 Tentang Pemberantasan Tindak Pidana Terorisme, karena dalam Pasal 63 ayat (1) KUHP disebutkan bahwa "jika suatu perbuatan masuk dalam lebih dari satu ketentuan pidana, maka yang dikenakan hanya salah satu diantara aturan-aturan itu; jika berbeda-beda, yang dikenakan yang memuat ancaman pidana pokok yang paling berat." (R. Indonesia, 2002).

Akan Tetapi Pada kenyataannya putusan dijatuhkan kepada tersangka hanya penjara 7 bulan dan tanpa denda padahal dalam melakukan kejahatan tersebut BBA meraup uang senilai Rp. 31,5 miliar. Sangat tidak

relevan dengan perbuatannya, maka dari itu harus ada fomulasi yang pas dalam penegakan tindak pidana *cyber crime* ini, karena dalam hal *cyber crime* telah bersifat *transnasional* yang dilakukan pelaku *cyber crime hacker* menggunakan *modus operandi.* Seharusnya dalam penegakan hukum dibidang *cyber crime hacker* kita harus menggunakan konsep *concursus* karena *cyber crime* dalam melakukan aksinya terdapat perbarengan tindak pidana supaya tercipta keadilan, kepastian, dan kemanfaatan hukum.

Kebijakan Formulasi Hukum Pidana Dalam Penanggulangan *Cyber Crime* di Masa Yang Akan Datang

Menjawab tuntutan dan tantangan komunikasi global lewat internet, undang-undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Penanggulangan terhadap tindak pidana teknologi informasi perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur, dan subtansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Barda Nawawi Arief menyatakan bahwa upaya melakukan pembaharuan hukum pidana pada hakikatnya termasuk bidang "penal policy" yang merupakan bagian dan terkait dengan *"law enforcement policy", "criminal policy", "social policy".* Ini berarti pembaharuan hukum pidana pada hakikatnya (Arief, 2011): 1) Merupakan bagian dari kebijakan (upaya rasional) untuk memperbaharui substansi hukum (*legal substansi*) dalam rangka lebih mengefektifkan penegakan hokum; 2) Merupakan bagian dari kebijakan (upaya rasional) untuk memberantas/ menanggulangi kejahatan dalam rangka perlindungan masyarakat; 3) Merupakan bagian dari kebijakan (upaya rasional) untuk mengatasi masalah sosial dan masalah kemanusiaan dalam rangka mencapai/menunjang tujuan nasional (yaitu *social defence dan social welfare*); 4) Merupakan upaya peninjauan dan penilaian kembali (reorientasi dan re-evaluasi) pokok-pokok pemikiran, ide-ide dasar, atau nilai sosio-filosofik, sosio politik dan sosio kultural yang melandasi kebijakan kriminal dan kebijakan (penegakan) hukum pidana selama ini. Bukanlah pembaharuan (reformasi) hukum pidana, apabila orientasi nilai dari hukum pidana yang dicitacitakan sama saja dengan orientasi nilai dari hukum pidana lama warisan penjajah (KUHP lama atau WvS) (Arief, 2011).

Bertolak dari kebijakan tersebut di atas, usaha dan kebijakan untuk membuat peraturan hukum pidana yang pada pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Dengan demikian penentuan kebijakan hukum pidana menanggulangi *cyber crime* harus dilakukan dengan pendekatan kebijakan dan di dalam setiap kebijakan (*policy*) terkandung pula pertimbangan nilai (Silaen & Siregar, 2020; Situmeang, 2022). Oleh karena itu, pembaharuan hukum pidana dalam penanggulangan tindak pidana teknologi informasi harus pula berorientasi pada pendekatan nilai. 1) Kebijakan formulasi tindak pidana. Hukum pidana merupakan salah satu sarana kebijakan kriminal untuk menanggulangi *cyber crime*. Dalam kebijakan hukum pidana, maka akan bersentuhan dengan persoalan kriminalisasi (*criminalization*), baik itu perbuatan yang melawan hukum *(actus reus*), pertanggungjawaban pidana (*mensrea*), maupun sanksi yang dijatuhkan berupa pidana (*punishment*) maupun tindakan (*treatment*); 2) Kebijakan kriminalisasi. Kriminalisasi harus memenuhi berbagai syarat antara lain bahwa perbuatan tersebut benar-benar menampakkan korban (*victimizing*), baik aktual maupun pontensial, kemudian konsistensi penerapan asas ultimum remedium, dukungan publik yang kuat, bersifat komprehensif dan tidak bersifat *adhoc* (Ali & Hafid, 2022; Muladi, 2003).

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana) (Zaidan & Sh, 2021). Jadi pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (*penal policy*), khususnya kebijakan formulasinya.

Berdasarkan uraian tersebut, maka ruang hukum dalam penyelesaian perkara tindak pidana *cyber crime* untuk kedepannya harus ada reformasi hukum dalam bidang *cyber crime* sehingga para pelaku *cyber crime* mendapatkan hukuman yang setimpal atas perbuatannya. Dan dalam kasus *cyber crime hacker* kita dapat menggunakan konsep *concursus* berupa sistem kumulasi diperlunak atau di sebut *concursus realis.* dengan cara pidana penjara terberat ditambahkan sepertiga dari masing-masing pidana terberat.

Simpulan

Penegakan hukum melalui pengungkapan tindak pidana, menemukan pelaku, serta memasukkan pelakunya ke dalam penjara (*follow the suspect*) semata belum efektif mengatasi perkembangan tindak pidana *cyber crime*

hacker jika hanya menggunakan pidana penjara terberat saja, tidak menggunakan konsep perbarengan tindak pidana (*concursus*). Proses pemidanaan pelaku *cyber crime hacker* masih sangat lemah jika dibandingkan dengan *efek negative* yang dapat ditimbulkannya, penegakan hukum belum terintegrasi dengan baik dengan *stake holden* di bidang *cyber* seperti badan sandi dan siber negara atau BSSN dan pemangku kepentingan lainnya.

Formulasi kebijakan hukum pidana melalui Undang-Undang Negara Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE mutlak diperlukan bagi negara Indonesia, karena saat ini Indonesia merupakan salah satu negara yang menggunakan dan memanfaatkan teknologi informasi secara luas dan efisien, dan secara faktual belum dapat mengakomodir perkembangan hukum *cyber*, terutama dari aspek hukum pidana.

Referensi

Ali, M., & Hafid, I. (2022). Kriminalisasi Berbasis Hak Asasi Manusia Dalam Undang-Undang Bidang Lingkungan Hidup. *Jurnal USM Law Review, 5*(1), 1-15.

Arief, B. N. (2011). Bunga Rampai Kebijakan Hukum Pidana:(Perkembangan Penyusunan Konsep KUHP Baru).

Ator, F. (2021). Pemidanaan Terhadap Pelaku Perbuatan Berlanjut Dalam Pasal 64 KUHP. *Lex Privatum, 9*(4).

Azra, H. A. (2022). Analisis Penerapan Concursus Realis dalam Pemidanaan terhadap Pelaku Penganiayaan dan Pemerasan (Studi Putusan Nomor: 533/Pid. B/2019/PN Tjk).

Handoko, D. (2018). *Kitab undang-undang hukum pidana*: Hawa dan AHWA.

Indonesia, P. R. (1981). Undang Undang No. 8 Tahun 1981 Tentang: Kitab Undang Undang Hukum Acara Pidana. *Sinar Grafika. jakarta*.

Indonesia, R. (2002). *Undang-undang dasar negara republik indonesia Tahun 1945*: Sekretariat Jenderal MPR RI.

Insani, N. (2022). The Implementation of Concursus Criminal Offense Sanctions Related to Article 12 Paragraph 4 of the Criminal Code. *Open Access Repository, 8*(05), 136-144.

Johan, N. B. (2016). *Metode Penelitian Hukum*. Bandung: Mandar Maju.

Keintjem, F. A. (2021). Konsep Perbarengan Tindak Pidana (Concurcus) Menurut Kitab Undang-Undang Hukum Pidana. *Lex Crimen, 10*(5).

Kusuma, W., & Khairina. (2019). Hacker Asal Sleman yang Retas Perusahaan AS Dikenal Pribadi Tertutup, from https://regional.kompas.com/read/2019/10/28/08372891/hacker-asal-sleman-yang-retas-perusahaan-as-dikenal-pribadi-tertutup.

Marzuki, P. M. (2013). Penelitian hukum.

Muladi. (2003, 23 Agustus 2003). Kebijakan Kriminal Terhadap Cybercrime. *Majalah Media Hukum Volume I No.3*.

Muladi, S., Diah Sulistyani, R., & SH, C. (2021). *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*: Penerbit Alumni.

Nurhayati, Y., Ifrani, I., & Said, M. Y. (2021). Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum. *Jurnal Penegakan Hukum Indonesia, 2*(1), 1-20.

Prakasa, D. L., & Astoni, P. Y. (2022). Analisis pertanggung jawaban penyidik polda metro jaya dalam kaitan terhadap terjadinya salah tangkap atau error in persona. *Jurnal Ilmiah Publika, 10*(2), 467-476.

Prasetyo, T. (2011). Hukum pidana.

Prodjodikoro, W. (2008). Tindak-tindak pidana tertentu di Indonesia. *(No Title)*.

Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal, 1*(2), 68-81.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Mimbar Jurnal Hukum, 2*(1), 58-77.

Silaen, F., & Siregar, S. A. (2020). Hubungan Kebijakan Kriminal Dengan Kebijakan Hukum Pidana. *Jurnal Darma Agung, 28*(1), 8-16.

Sitepu, K. A. B., Lubis, Y., & Sahlepi, M. A. (2023). Peran penyidik dalam mengungkap pelaku tindak pidana pembunuhan berencana disertai dengan mutilasi (studi di kepolisian daerah Sumatera Utara). *Jurnal Meta Hukum, 2*(3), 63-76.

Situmeang, S. M. T. (2022). Politik Hukum Pidana terhadap Kebijakan Kriminalisasi dan Dekriminalisasi dalam Sistem Hukum Indonesia. *Res Nullius Law Journal, 4*(2), 201-210.

Tarmizi, D. T. D. (2022). Jurnal Kebijakan Penegakan Hukum Pidana Terhadap Perbarengan Perbuatan Pidana (Concursus Realis): Kebijakan Penegakan Hukum Pidana Terhadap Perbarengan Perbuatan Pidana (Concursus Realis). *Hangoluan Law Review, 1*(1), 69-105.

Undang-Undang. (2016). Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Zaidan, M. A., & Sh, M. (2021). *Kebijakan Kriminal*: Sinar Grafika (Bumi Aksara).