ALTERNATIF PIDANA BAGI PELAKU TINDAK PIDANA PERETASAN DI INDONESIA DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Asfarina Oktaviani
Program Studi S-1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya,
asfarinaoktaviani16040704114@mhs.unesa.ac.id

Emmilia Rusdiana
Program Studi S-1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya,
emmiliarusdiana@unesa.ac.id

Abstrak

Tindak pidana peretasan merupakan akar dari *cybercrime* terhadap kerahasiaan, integritas, ketersediaan sistem informasi dan elektronik maupun dokumen elektronik. Peretas tentu memiliki peranan yang sangat penting dalam rangka pembangunan internet. Mereka melakukan pengujian terhadap sistem untuk memperoleh hasil yang memiliki standar baik dalam penggunaan internet, mengembangkan kemampuannya untuk menjaga serta meningkatkan keamanan siber pada situs-situs resmi perusahaan hingga pemerintahan agar terhindar dari ancaman peretasan lainnya yang dapat merugikan negara. Ketentuan sanksi pidana di Indonesia yang dapat diancamkan bagi peretas nyatanya belum efektif untuk mengurangi angka *cybercrime* di Indonesia. Penelitian ini bertujuan untuk mengidentifikasi pengaturan tindak pidana peretasan di Indonesia serta mengidentifkasi dan menganalisis bentuk alternatif pidana bagi pelaku tindak pidana peretasan di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan menggunakan pendekatan perundang-undangan, pendekatan historis, pendekatan komparatif, dan pendekatan konseptual. Teknik analisis data penelitian adalah kualitatif. Hasil penelitian menunjukkan bahwa pengaturan tindak pidana peretasan di Indonesia secara historis pertama kali diatur dalam Undang-Undang No 3 tahun 1989 tentang Telekomunikasi yaitu Pasal 23 dan Pasal 35, kemudian diatur dalam Pasal 22 *jo* Pasal 50 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi dan terakhir diatur dalam Pasal 30 *jo* Pasal 46 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Alternatif pidana bagi peretas telah diberlakukan di Belanda dan Uzbekistan, maka dimungkinkannya di Indonesia juga menerapkan alternatif pidana yang efektif bagi para peretas seperti pidana pengawasan dan pidana kerja sosial dengan mempertimbangkan potensi dan keahlian yang dimiliki pelaku dalam hal teknologi.
Kata Kunci: *Cybercrime*, peretasan, alternatif pidana

Abstract

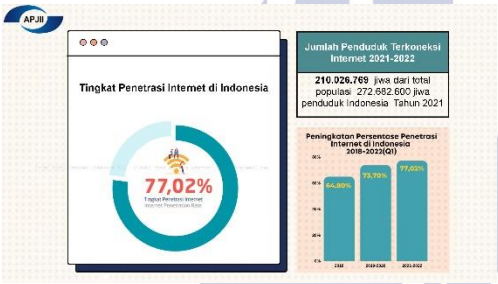
The criminal act of hacking is the root of cybercrime against confidentiality, integrity, availability of information systems and electronics and electronic documents. Hackers certainly have a very important role in the framework of internet development. They carry out tests on the system to obtain results that have good standards in internet use, develop its ability to maintain and improve cybersecurity on official corporate to government websites to avoid other hacking threats that can harm the state. Provisions for criminal sanctions in Indonesia that can threaten hackers are in fact not yet effective in reducing the number of cybercrimes in Indonesia. This study aims to identify the regulation of criminal acts of hacking in Indonesia as well as to identify and analyze alternative forms of punishment for perpetrators of criminal acts of hacking in Indonesia. The research method used is normative juridical using statutory approaches, historical approaches, comparative approaches, and conceptual approaches. Research data analysis technique is qualitative. The results of the study show that the regulation of criminal acts of hacking in Indonesia historically was first regulated in Law No. 3 of 1989 concerning Telecommunications, namely Article 23 and Article 35, then regulated in Article 22 in conjunction with Article 50 of Law Number 36 of 1999 concerning Telecommunications and the latter is regulated in Article 30 in conjunction with Article 46 of Law Number 11 of 2008 concerning Information and Electronic Transactions. Criminal alternatives for hackers have been implemented in the Netherlands and Uzbekistan, so it is possible in Indonesia to also implement effective criminal alternatives for hackers such as supervision punishment and social work punishment by taking into account the potential and expertise possessed by the perpetrators in terms of technology.

Keywords: Cybercrime, hacking, alternative punishment

PENDAHULUAN

Pada era globalisasi saat ini, perkembangan teknologi informasi dan komunikasi di berbagai bidang mengalami kemajuan yang sangat pesat dan memberikan kontribusi signifikan terhadap perkembangan zaman yang semakin modern ini. Teknologi Informasi seringkali disamakan dengan internet. Kemunculan internet sendiri begitu fenomenal. Dengan adanya internet tersebut telah berhasil menghilangkan semua batas-batas fisik yang memisahkan manusia dan menyatukannya dalam sebuah dunia yang baru, yaitu "dunia maya". Interaksi secara *virtual* memudahkan masyarakat untuk tetap terhubung dengan yang lainnya maka hal ini mengakibatkan pengguna internet di dunia mengalami peningkatan.

Gambar 1.1 Data Penetrasi Pengguna Internet di Indonesia tahun 2021-2022



Sumber: Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2021-2022

Berdasarkan hasil survey tersebut, maka diketahui bahwasannya pengguna internet di Indonesia dari tahun ke tahun telah mengalami peningkatan yang cukup signifikan. Peningkatan mulai dari tahun 2018 ke tahun 2019-2020 yaitu sebesar 8,90%, peningkatan dari tahun 2019-2020 ke tahun 2021-2022 yaitu sebesar 3,32%. Kemudahan akses perangkat elektronik ke jaringan internet dan banyaknya jumlah perangkat elektronik yang dapat tersambung internet dapat menjadi salah satu faktor pertumbuhan pengguna internet di Indonesia akan terus meningkat.

Peningkatan jumlah pengguna internet dan perkembangan teknologi informasi telah membuat dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Perubahan yang ditimbulkan oleh meningkatnya perkembangan teknologi informasi ini dapat membawa manfaat bagi masyarakat karena memberikan kemudahan dalam berbagai aktivitas terutama yang terkait dengan pemanfaatan informasi. Namun disisi lain, hal tersebut memicu timbulnya berbagai bentuk konflik dimasyarakat sebagai akibat dari penggunaan yang tidak bertanggung jawab. Kejahatan tersebut disebut juga dengan *Cybercrime*, *Cybercrime* merupakan aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan (Ramli 2006).

Pengaturan tindak pidana siber dalam peraturan perundang-undangan Indonesia belum cukup respresentatif dan harmonis. Hal ini memiliki implikasi baik terhadap hukum pidana materil maupun hukum pidana formil (Suseno 2012). Berbagai upaya untuk mengatur pengaturan pada peraturan perundang-undangan yang dapat mencegah adanya dampak negatif akibat dari perbuatan hukum harus segera dilakukan dan untuk menghukum pelaku tindak pidana. Kitab Undang-Undang Hukum Pidana (KUHP) sebagai *lex generalis* bagi aturan hukum materiil pada kenyataannya tidak dapat digunakan untuk menjerat hukuman pada pelaku kejahatan terbaru. Dengan disahkannya Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada bulan Maret 2008 dan Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) sebagai *lex specialis* bagi aturan hukum materiil diluar KUHP yang didalamnya mengatur mengenai tindak pidana yang merugikan kepentingan hukum yang dilakukan menggunakan media Teknologi Informasi dan Komunikasi sebagai sarana untuk melancarkan aksi kejahatannya, seperti peretasan (*hacking*).

Gambar 1.2 Jumlah Akun yang telah Diserang Q3-2022

Negara	Total pengguna yang dilanggar
Rusia	22,3 Juta
Perancis	13,8 Juta
Indonesia	13,3 Juta
Amerika Serikat	8,5 Juta
Spanyol	3,9 Juta

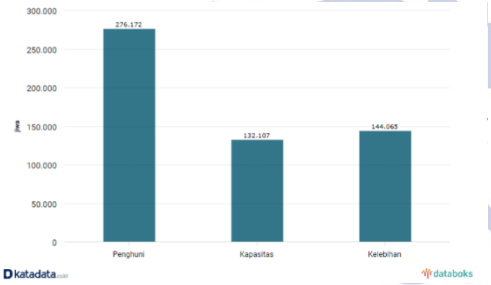
Sumber: Surfshark - Data breaches rise globally in Q3 of 2022

Kesimpulannya, Indonesia telah menduduki peringkat ketiga mengenai jumlah kasus kebocoran data terbanyak di dunia pada tahun 2022 yaitu dengan jumlah 13,8 juta akun yang telah berhasil bocor. Data tersebut semakin memperkuat bukti bahwa Indonesia masih sangat rentan terkena serangan siber. Peningkatan serangan siber ini terjadi selain kurangnya *self-awareness* setiap pengguna atas pentingnya menjaga data pribadi pada setiap akun dan juga diidentifikasi sebagai akibat dari semakin canggihnya serangan yang dikembangkan oleh pelaku *cybercrime*. Pengamat masalah militer LIPI, Jaleswari Pramodhawardani juga berpendapat bahwa Indonesia memiliki peretas-peretas tangguh yang sangat dibutuhkan

untuk membentuk satuan tentara siber (*cyber army*). Melalui merekalah penanganan kriminalitas siber dapat dilakukan. “Momentum ini sangat tepat dan kebijakan tersebut sangat penting, mengingat ancaman di dunia maya terhadap pertahanan negara semakin besar” (R24 2017).

Kasus *cybercrime* terkhususnya dalam hal peretasan dapat diibaratkan seperti sebuah gunung es ditengah samudera. Hanya sebagian kecil dari bagian gunung es tersebut yang dapat dilihat, sedangkan hal yang tersembunyi di bawah permukaan laut lebih besar berkali kali lipat dibandingkan yang terlihat di permukaan. Jika dilihat dari sudut pandang tindak pidana, peretas pada beberapa kasus di atas harus ditetapkan sebagai pelaku yang telah melakukan sebuah tindak pidana karena perbuatan tersebut merupakan tindakan yang melawan hukum yaitu melakukan peretasan situs-situs sehingga situs tersebut tidak dapat difungsikan secara normal dalam beberapa waktu, mengalami kebocoran data dan kerugian-kerugian lainnya karena akibat dari peretasan dan pemerasan. Pelaku dapat diancam dengan sanksi dan dianggap orang yang dapat bertanggungjawab atas perbuatan tersebut. Sudah sewajarnya, tindakan pelaku untuk dijatuhi hukuman atau sanksi pidana. Namun, penjatuhan sanksi pidana penjara dan/atau denda kurang efektif karena melihat kondisi Rutan dan Lapas di Indonesia sudah sangat mengkhawatirkan.

Gambar 1.3 Penghuni Lapas di Seluruh Indonesia September 2022



Sumber: Databoks - Penghuni Lapas di Seluruh Indonesia (19/9/2022)

Berdasarkan data Dirjen Pemasyarakatan Kementerian Hukum dan HAM September 2022, beban Rutan dan Lapas di Indonesia mencapai 209% dengan jumlah 144.065 orang. Jumlah penghuni Rutan dan Lapas di Indonesia mencapai 276.172 orang. Padahal, kapasitas Rutan dan Lapas hanya dapat menampung 132.107 orang. Sedangkan data dari Yosua Octavian anggota Koalisi Pemantau Peradilan, sebelum kebijakan asimilasi untuk pencegahan penyebaran *Covid*-19, pada Maret 2020 jumlah penghuni Rutan dan Lapas di Indonesia mencapai 270.466 orang dari total kapasitas sebanyak 132.335 orang Beban Rutan dan Lapas di Indonesia mencapai 204% (Muhammad and Kuswandi 2020). Kesimpulannya, beban Rutan dan Lapas di Indonesia pada tahun 2022 telah mengalami peningkatan sebesar 5% dalam kurun waktu 2 tahun (2020-2022). Kondisi tersebut telah mencapai *extreme overcrowding* karena perbandingan tahanan dan kapasitas melebihi 150 persen. Sementara, jumlah tahanan dan narapidana selama 5 tahun terakhir tidak mengalami penurunan (Erdianto 2018). Kelebihan kapasitas penghuni penjara merupakan suatu hal yang tidak manusiawi bagi narapidanna dan hal itu dapat juga diartikan bahwa negara juga menanggung beban biaya lebih banyak untuk kebutuhan hidup narapidana di penjara. Penjara merupakan tempat yang paling tidak efektif digunakan sebagai tempat untuk memulihkan para narapidana, telah menjadi rahasia umum bahwa saat berada dalam penjara dapat meningkatkan kemungkinan narapidana untuk melakukan suatu pelanggaran lainnya. Beberapa alasan mengenai hal tersebut yaitu ketidakmampuan para narapidana untuk berfungsi dalam lingkungan sosial akibat dari trauma penahanan dan telah terbiasa akan terisolasinya diri dari dunia luar karena saat berada di penjara, gaya hidup para narapidana akan diatur dan dibatasi berbeda saat menjalani kehidupan normal di luar penjara. Meskipun penjara dianggap sebagai salah satu pilar paling hebat untuk menjamin ketertiban sosial, penjara tidak menjadi penghalang bagi narapidana untuk melakukan pelanggaran lainnya dan juga dikhawatirkan narapidana akan saling bertukar ilmu untuk memperluas pengetahuan dalam hal kejahatan yang mendorong narapidana lain akan melakukan kejahatan-kejahatan lain dengan lebih baik.

Hukum pidana harus selalu sejajar dengan perkembangan teknologi yang dapat menawarkan berbagai kesempatan kepada pelaku untuk menyalahgunakan fasilitas-fasilitas yang terdapat dalam *cyberspace* dan menyebabkan kerugian bagi para pihak yang berkepentingan (Sitompul Josua 2021). Terlepas dari kontroversi perbuatan yang dilakukan peretas terhadap perkembangan teknologi informasi, pada saat ini peretas memiliki peranan yang sangat penting dalam rangka pembangunan internet. Mereka melakukan pengujian terhadap sistem untuk memperoleh hasil yang memiliki standar baik dalam penggunaan internet (Hardinanto Aris 2019). Pemidanaan bagi pelaku *cybercrime* khususnya pelaku peretas situs menjadi kurang efektif jika hanya dijatuhi hukuman pidana penjara dan/atau denda, melihat potensi yang dimiliki peretas seperti penjelasan sebelumnya serta dapat mengembangkan kemampuannya dalam hal menjaga dan meningkatkan keamanan siber pada situs-situs resmi pemerintahan agar terhindar dari ancaman peretasan lainnya yang dapat merugikan negara.

Berdasarkan latar belakang di atas, maka dapat dirumuskan beberapa permasalahan yang akan dibahas

dalam penelitian ini yaitu bagaimana pengaturan tindak pidana peretasan di Indonesia serta bagaimana bentuk alternatif pidana bagi pelaku tindak pidana peretasan di Indonesia.

METODE

Jenis penelitian yang digunakan dalam penelitian ini adalah jenis penelitian yuridis normatif (*legal research*). Penelitian yuridis normatif merupakan penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif. Selain itu, penelitian hukum normatif juga dapat diartikan sebagai penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka dalam penelitian ini akan mengkaji ketentuan tentang tindak pidana peretasan dalam UU ITE dan alternatif pidana.

Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*), pendekatan historis (historical approach), pendekatan konseptual (*conseptual approach*) dan pendekatan komparatif (*comparative approach*). Pendekatan perundang-undangan (*statute approach*) dilakukan dengan cara menelaah semua ketentuan peraturan perundang-undangan terkait dengan peretasan di Indonesia dan beberapa negara yang akan diteliti. Pendekatan historis dalam penelitian ini dilakukan untuk mengidentifikasi sejarah mengenai pengaturan tindak pidana peretasan di Indonesia. Pendekatan konseptual dalam penelitian ini bersumber dari pandangan-pandangan dan doktrin-doktrin yang berkembang mengenai hukum pidana, *cybercrime*, sistem pemidanaan, alternatif pidana dan tujuan pemidanaan yang menjadi sandaran dalam membangun argumentasi untuk memecahkan isu hukum yang diteliti.

Pendekatan komparatif dilakukan dengan mengadakan studi perbandingan hukum. Menurut Gutteridge, perbandingan hukum merupakan suatu metode studi dan penelitian hukum. Studi perbandingan hukum juga merupakan kegiatan untuk membandingkan hukum suatu negara dengan hukum negara lain, disamping itu juga membandingkan suatu putusan pengadilan yang satu dengan putusan pengadilan lainnya untuk masalah yang sama. Dalam penelitian ini, akan membandingkan ketentuan tindak pidana peretasan dalam peraturan perundang-undangan di Indonesia, Belanda serta Uzbekistan.

Sumber bahan hukum yang digunakan pada penelitian ini yaitu bahan hukum primer, sekunder dan tersier.

a. Bahan Hukum Primer

Bahan hukum primer adalah bahan hukum autoritatif yang terdiri dari perundang-undangan, dan putusan hakim. (Ali 2009) Bahan hukum primer yang digunakan dalam penelitian ini terdiri dari:

1) *Wetboek van strafrecht* (WvS)
2) *Criminal Code of the Republic of Uzbekistan*
3) Undang-Undang Nomor 3 tahun 1989 tentang Telekomunikasi
4) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi sebagai pengganti Undang-Undang Nomor 3 tahun 1989 tentang Telekomunikasi
5) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
6) Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
7) *United Nations Standard Minimum Rules for Non-custodial Measures (The Tokyo Rules)*
8) *Convention on Cybercrime* tahun 2001

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan terhadap bahan hukum primer yakni hasil karya para ahli hukum yang terdapat dalam buku-buku teks hukum yang berkaitan dengan hukum pidana, sistem pemidanaan, politik hukum pidana, *cybercrime*, prinsip-prinsip dasar hukum pidana (asas hukum pidana), jurnal-jurnal hukum terkait dengan hukum pidana, sistem pemidanaan *cybercrime*, data *cybercrime* terkhususnya terkait peretasan dan hasil penelitian yang berkaitan dengan topik penelitian.

c. Bahan Non-Hukum

Bahan-bahan non hukum berupa buku-buku mengenai keilmuan non hukum, laporan-laporan penelitian non hukum dan jurnal-jurnal non hukum, selama mempunyai relevansi dengan topik penelitian. Bahan-bahan non hukum tersebut bertujuan untuk menunjang, memperkaya dan memperluas wawasan peneliti (Marzuki 2005). Bahan non hukum yang akan digunakan dalam penelitian ini berupa buku, kamus, hasil penelitian dan jurnal berkaitan dengan peretasan.

Teknik pengumpulan bahan hukum dalam penelitian ini yaitu studi penelitian hukum (*legal research*) yang merupakan pengumpulan data sesuai dengan pendekatan dalam penelitian hukum. Pengumpulan bahan hukum yang sesuai dengan teknik pendekatan yang digunakan dalam penelitian ini adalah dengan cara membaca, mengkualifikasi dan mengidentifiksi aturan hukum yang kemudian membandingkan ketentuan mengenai tindak pidana peretasan dari 3 negara berbeda. Data-data tersebut kemudian dianalisis dan dirumuskan sebagai data penunjang di dalam penelitian ini.

Bahan hukum yang telah dikumpulkan, kemudian bahan hukum tersebut diolah secara sistematis untuk mendapatkan gambaran yang utuh dan jelas tentang permasalahan yang akan dibahas. Pengolahan bahan dalam penelitian hukum normatif dilakukan dengan cara melakukan seleksi bahan hukum kemudian melakukan

klasifikasi menurut penggolongan bahan hukum dan menyusun data hasil penelitian tersebut secara sistematis, tentu saja hal tersebut dilakukan secara logis, dalam artian ada hubungan dan keterkaitan antara bahan hukum satu dengan bahan hukum lainnya untuk mendapatkan gambaran umum dari hasil penelitian (Marzuki 2005).

Teknik analisis bahan hukum dengan menggunakan analisis preskriptif yang dilakukan dengan cara mengumpulkan serta mengelompokkan bahan hukum primer dan bahan hukum sekunder kemudian dianalisis dengan menggunakan pendekatan penelitian yang digunakan, setelah itu dilakukannya identifikasi aturan hukum dan mengeliminasi hal-hal yang tidak relevan, memecahkan isu hukum yang telah teridentifikasi dengan menggunakan reskontruksi hukum berdasarkan pendekatan yang telah ditentukan sebelumnya.

HASIL DAN PEMBAHASAN

A. Pengaturan Tindak Pidana Peretasan di Indonesia

Secara historis, sistem hukum pidana di Indonesia hingga saat ini mengacu pada sistem hukum pidana kolonial Belanda. KUHP dan KUHAP yang merupakan induk dari aturan hukum pidana dan acara pidana di Indonesia masih belum mampu menangani *cybercrime* atau kejahatan lain yang muncul di dunia maya. Aturan-aturan konvensional tidak lagi dapat digunakan untuk mengatasi *cybercrime* (Suhariyanto 2013). Pada tahun 1988, pertama kali diadakan suatu kajian terhadap *cybercrime* dan KUHP di Indonesia saat Departemen Kehakiman dan Badan Pembinaan Hukum Nasional (BPHN) mengadakan sebuah acara diskusi dengan tema "Kejahatan Komputer" dengan narasumber dari Belanda, yaitu Prof. Nico Keijzer (anggota Mahkamah Agung Belanda), Prof. Dieter chaffmeister (Guru Besar Hukum Pidana Universitas Leiden) serta Mr. P.H. Sitorius (advokat). Pihak Belanda membawakan makalah dengan judul "Hukum Pidana dan Penyalahgunaan Komputer" dan pihak Indonesia yang diwakili oleh Prof. Boy Mardjono Reksodiputro membawakan makalah dengan judul "Kejahatan Komputer". Prof. Boy Mardjono Reksodiputro berpendapat bahwa perlu ditambahkan "pengaman" berupa ketentuan mengenai kejahatan komputer di dalam KUHP. Salah satu contoh perbuatan tersebut yaitu *unauthorized access* (akses ilegal) (Hardinanto Aris 2019).

Undang-Undang No 3 tahun 1989 tentang Telekomunikasi menjadi undang-undang pertama di Indonesia yang mengatur tentang *cybercrime*, yaitu tercantum dalam Pasal 23 dan Pasal 35 yang berbunyi:

Pasal 23

"Perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dilarang."

Pasal 35

"Setiap perbuatan yang dilakukan tanpa hak dan dengan sengaja untuk mengubah jaringan telekomunikasi dan/atau memanipulasi penyelenggaraan telekomunikasi sehingga menimbulkan kerugian pada penyelenggara atau pun pemakai jasa telekomunikasi merupakan tindak pidana."

Berdasarkan penjelasan Pasal 23, Perbuatan-perbuatan yang dapat menimbulkan gangguan terhadap penyelenggaraan telekomunikasi dapat berupa:

"a. tindakan fisik yang menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;
b. tindakan fisik yang mengakibatkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;
c. penggunaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;
d. penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelenggaraan telekomunikasi lainnya;
e. penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki terhadap suatu penyelenggaraan telekomunikasi."

Sedangkan menurut penjelasan Pasal 35, yang berbunyi:

"Ketentuan ini dimaksudkan untuk melindungi penyelenggaraan jasa telekomunikasi dan pemakai jasa telekomunikasi dari perbuatan-perbuatan yang dapat menimbulkan kerugian baik yang dilakukan oleh penyelenggara jasa telekomunikasi, pemakai jasa, atau pun pihak-pihak lainnya seperti pencantolan sambungan telepon, pemasangan nomor ganda, memanipulasi pulsa, dan lain-lainnya. Penggunaan sarana telekomunikasi oleh siapa pun yang menyimpang dari ketentuan yang berlaku merupakan tanggungjawab sepenuhnya dari pihak yang menggunakannya."

Berdasarkan penjelasan Pasal 23 dan Pasal 35 di atas, maka dapat diketahui unsur-unsur yaitu unsur menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi, unsur tanpa hak dan sengaja, unsur mengubah jaringan telekomunikasi dan/atau memanipulasi penyelenggaraan telekomunikasi serta unsur menimbulkan kerugian pada penyelenggara atau pun pemakai jasa telekomunikasi. Maka disimpulkan bahwa jenis perbuatan *cybercrime* yang diatur dalam Undang-Undang No 3 tahun 1989 tentang Telekomunikasi adalah *illegal interception* atau penyadapan terhadap aktivitas telekomunikasi yang

mengakibatkan kegiatan telekomunikasi menjadi terhambat.

Disahkannya Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi sebagai pengganti Undang-Undang Nomor 3 tahun 1989 tentang Telekomunikasi dengan alasan yang telah tercantum dalam konsideran, yaitu pengaruh globalisasi dan perkembangan teknologi telekomunikasi yang dangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi. Dalam undang-undang ini telah mengenal adanya perbuatan peretasan yaitu diatur dalam Pasal 22 *jo* Pasal 50 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi yang mengatur bahwa:

Pasal 22

"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:
a. akses ke jaringan telekomunikasi; dan atau
b. akses ke jasa telekomunikasi; dan atau
c. akses ke jaringan telekomunikasi khusus."

Pasal 50

"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyakRp600.000.000,00 (enam ratus juta rupiah)."

Namun seiring berjalannya waktu, undang-undang tersebut tidak dapat mengatasi seluruh permasalahan yang timbul akibat perkembangan teknologi, mengingat bahwa secara yuridis segala bentuk kegiatan dalam ruang siber tidak dapat dicapai hanya dengan menggunakan ukuran dan kulifikasi hukum konvensional karena kegiatan dalam ruang siber merupakan kegiatan *virtual* yang dapat berdampak secara nyata dan nantinya akan banyak kesulitan serta kemungkinan lolos dari pemberlakuan hukum, walaupun pada kenyataannya masyarakat (manusia) yang hidup di dunia nyata masih tetap dilibatkan.

Pada bulan Maret 2003, Kementerian Negara Komunikasi dan Informatika mulai membahas Rancangan Undang-Undang Informasi dan Transaksi Elektronik dan akhirnya disahkan pada tanggal 28 April 2008. Berlakunya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang secara umum mengatur tentang apa saja mengenai data elektronik dan pemanfaatannya bagi kepentingan umum yang diharapkan dapat mengatasi permasalahan terkini yang berkaitan dengan aktivitas di dunia maya. Terdapat 2 hal penting yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin serta diklasifikasikannya tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan teknologi informasi disertai sanksi pidananya termasuk untuk tindakan *carding*, *hacking* dan *cracking* (Kemenkumham n.d.).

Pengertian akses menurut Pasal 1 angka 15 UU ITE merupakan kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan. Akses dengan sistem elektronik yang berdiri sendiri dalam bentuk fisik yaitu seperti menggunakan komputer maupun akses menggunakan aplikasi internet. Aturan mengenai *hacking* dalam UU ITE dijelaskan lebih rinci yaitu terdapat dalam Pasal 30 *jo* Pasal 46 mengatur bahwa:

Pasal 30

"(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 46

"(1) Setiap orang yang memenuhi unsur sebaagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)
(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)
(3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)"

Pasal 30 UU ITE di atas mengacu pada *Article 2 Convention on Cybercrime*, yang mengatur bahwa (Council of Europe 2001):

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Terjemahan:

"Setiap pihak harus mengambil langkah-langkah legislatif dan langkah-langkah lain yang mungkin diperlukan untuk ditetapkan sebagai tindak pidana berdasarkan undang-undang nasionalnya, ketika dilakukan dengan sengaja, akses ke seluruh atau sebagian sistem komputer tanpa hak. Suatu Pihak dapat meminta agar kejahatan dilakukan dengan melanggar langkah-langkah keamanan, dengan maksud memperoleh data komputer atau maksud tidak jujur lainnya, atau dalam kaitannya dengan sistem komputer yang terhubung ke sistem komputer lain."

Sebagai bagian dari masyarakat dunia, Indonesia mutlak berperan serta secara aktif dalam berbagai aspek pergaulan dunia internasional. Salah satu aspek yang saat ini tengah dihadapi dunia internasional yaitu upaya pemberantasan terhadap *cybercrime*. Mengingat karakteristik *cybercrime* yang bersifat *borderless* dan menggunakan teknologi tinggi sebagai media, maka kebijakan kriminalisasi di bidang teknologi informasi harus memperhatikan perkembangan upaya penanggulangan *cybercrime*, baik regional maupun internasional dalam rangka harmonisasi dan uniformitas pengaturan *cybercrime*, seperti EU *Convention on Cybercrime* 2001 yang telah dibuat pada tanggal 23 November 2001 di Kota Budapest, Hungaria oleh negara-negara yang tergabung dalam Uni Eropa (*Council of Europe*) (Suparni Niniek 2009).

Isi Pasal 30 di atas, terdapat 3 jenis kategori perbuatan yang dilarang dengan cara meretas, yaitu:

1. Peretasan secara umum yang dilakukan dengan cara apapun
2. Peretasan dengan tujuan untuk mendapatkan informasi elektronik dan/atau dokumen elektronik
3. Peretasan dengan cara melumpuhkan sistem keamanan

Isi dari Pasal 30 ayat (1) UU ITE memberikan perlindungan hukum terhadap properti dan privasi seseorang, dengan cara melarang seseorang yang tidak memiliki hak atau kewenangan untuk mengakses komputer dan/atau sistem elektronik milik orang lain. Suatu komputer dan/atau sistem elektronik yang didalamnya berisikan ruang siber terdapat berbagai informasi dan dokumen elektronik yang dibuat atau diperoleh pemiliknya, merupakan ruang yang telah diciptakan dan dibatasi dari ruang siber yang lainnya berdasarkan kepentingan dan kontrol seseorang (pemilik). Maka, hanya si pemiliklah yang dapat mengakses dan mengontrol komputer atau sistem elektroniknya. Ia juga berhak untuk memperbolehkan dan melarang siapapun untuk mengakses komputer dan/atau sistem elektroniknya. Sedangkan orang lain bukan pemilik wajib menghormati privasi serta properti si pemilik, sehingga dilarang untuk mengakses komputer dan/atau sistem elektronik tanpa izin.

Namun, Pasal 30 ayat (1) UU ITE tidak mengatur tentang tujuan dan motif seseorang dalam mengakses komputer dan/atau sistem elektronik. Motivasi seseorang untuk melakukan peretasan tidak hanya untuk memperoleh keuntungan baik secara materil seperti uang dan informasi, tetapi juga keuntungan immaterial seperti status, ego, tantangan atau hiburan. Maka dari itu, berdasarkan ketentuan dalam Pasal 30 ayat (1) UU ITE melakukan peretasan tanpa hak merupakan perbuatan yang dilarang. Selain itu, tidak terdapat ketentuan yang membatasi cara seseorang untuk dapat mengakses komputer dan/atau sistem elektronik karena secara teknis terdapat begitu banyak cara untuk dapat mengakses komputer dan/atau sistem elektronik dan cara-cara tersebut tentunya akan semakin bervariasi sejalan dengan perkembangan teknologi. Maka dari itu, dalam UU ITE telah mengatur secara luas dengan menggunakan unsur "dengan cara apapun" (Sitompul Josua 2021).

Peretasan dapat dikatakan sebagai tindak pidana yang mengawali terjadinya tindak pidana yang lainnya karena hanya dengan mengakses komputer dan/atau sistem elektronik seseorang dapat mengambil alih kontrol atas sistem tersebut dan melakukan kejahatan lain. Pasal 30 ayat (2) UU ITE merupakan delik kualifisir (dikhususkan) dari ayat sebelumnya dengan ditambahkan unsur tujuan dari dilakukannya peretasan yaitu untuk memperoleh informasi dan/atau dokumen elektronik yang bersifat pribadi, rahasia, penting atau ekonomis. Dalam hal ini memang harus dijelaskan terlebih lanjut mengingat ketika seseorang telah berhasil mengakses secara sengaja ataupun tidak, informasi dalam komputer dan/atau sistem elektronik akan tampil dengan sendirinya (Suhariyanto 2013). Oleh karena itu, merujuk pada penjelasan Pasal 30 ayat (2) UU ITE, menjelaskan bahwa:

"Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
b. sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah."

Berdasarkan hal tersebut, maka ketentuan dalam Pasal 30 ayat (2) UU ITE ditujukan bagi perbuatan yang lebih serius dari sekedar mengakses suatu komputer dan/atau sistem elektronik secara tanpa izin, sehingga ancaman terhadap ketentuan ini juga diperberat. Pasal 30 ayat (3) UU ITE juga merupakan delik kualifisir (dikhususkan)

dari Pasal 30 ayat (1) UU ITE. Dua hal yang ditekankan dalam Pasal 30 ayat (2) UU ITE yaitu:

1. Dengan cara apapun
2. Dengan melanggar, menerobos, melampaui, atau menjebol

Terdapat penekanan pada bagian pertama yaitu "dengan cara apapun" ditujukan terhadap perbuatan mengakses komputer dan/atau sistem elektronik, sedangkan bagian kedua yaitu "melanggar, menerobos, melampaui atau menjebol" ditujukan kepada sistem pengamanan. Artinya, sebelum pelaku dapat mengakses komputer dan/atau sistem elektronik, ia harus melewati sistem pengamanan yang terdapat dalam komputer dan/atau sistem elektronik milik korban dengan cara melanggar, melampaui, menerobos atau menjebolnya. Unsur pada bagian kedua ini bersifat alternatif yang memiliki esensi yang sama dengan berhasil masuk ke dalam komputer dan/atau sistem elektronik dengan berhasil melalui sistem pengamanannya. Makna dari berhasil "melalui" sistem pengaman (menerobos atau menjebol) dan juga tanpa merusak sistem pengaman (melanggar atau melampaui) (Sitompul Josua 2021). Dalam hal ini, sistem pengamanan dijelaskan dalam Penjelasan Pasal 30 ayat (3) UU ITE, yang berisi:

> "Sistem pengamanan adalah sistem yang membatasi akses Komputer atau melarang akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan."

Penerapan sistem keamanan informasi sangat bervariasi, seperti dari yang paling sederhana seperti menggunakan kode akses hingga hal yang paling kompleks seperti mengatur konfigurasi jaringan komputer dan internet. Tentunya membutuhkan biaya yang bervariatif dalam penerapan sistem keamanan informasi. Semakin kompleks sistem yang dibangun maka semakin tinggi biaya yang harus dikeluarkan.

Karakteristik aktivitas pada ruang siber yang sifatnya lintas batas membuat manusia dapat masuk ke dalam dunia baru (dunia maya) yaitu melalui jaringan komputer dan sistem data yang kemudian menciptakan suatu perasaan bahwa mereka telah memasuki dunia baru yang tidak memiliki ketertarikan sama sekali dengan dunia nyata. Dengan kata lain, kebebasan yang diberikan saat beraktivitas dalam dunia maya membuat potensi *cybercrime* akan semakin meningkat. Pelaku *cybercrime* merasa aman dan terlindungi di balik anonimitas mereka dalam dunia maya. Adanya perbedaan prinsipil antara dunia nyata dan dunia maya yaitu, teknologi sebagai media yang digunakan yang menyebabkan seluruh interaksi dan aktivitas melalui internet akan berdampak bagi kehidupan bermasyarakat pada dunia nyata. Maka landasan pemikiran inilah yang mendasari disahkannya Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang masih berlaku hingga saat ini merupakan upaya negara untuk mengatasi kejahatan dunia maya.

B. Bentuk Alternatif Pidana bagi Pelaku Tindak Pidana Peretasan di Indonesia

Istilah "alternatif pidana" dan hukuman *non-custodial* telah lama digunakan secara bergantian untuk mencerminkan karakteristik umum dari rangkaian sanksi yang dilaksanakan di luar penjara. Secara historis, kualifikasi lebih lanjut harus dibuat karena setiap pengetahuan dalam perkembangan historis dari sanksi seperti kerja sosial, denda mengungkapkan bahwa sanksi semacam ini dalam berbagai bentuk ada pada periode awal sejarah, di mana penjara digunakan untuk orang-orang yang menunggu persidangan dan hukuman mereka. Penjara bukan hanya alternatif yang manusiawi untuk berbagai bentuk hukuman mati dan fisik, tetapi juga yang lebih penting bagaimana metode untuk melumpuhkan pelaku sekaligus memberikan efek jera yang lebih kuat dan bertahan lama.

Alternatif hukuman penjara mengacu pada tanggapan atau langkah-langkah yang dirancang untuk mengurangi penggunaan penjara dalam beberapa tahap dalam sistem peradilan pidana. Sejalan dengan definisi di atas, *United Nations Standard Minimum Rules for Non-Custodial Measures* atau dikenal dengan *Tokyo Rules* menggunakan istilah "*non-custodial measures*". Istilah ini mengacu pada keputusan yang diambil oleh pejabat yang berwenang dalam tahapan sistem peradilan pidana yang mewajibkan seseorang yang diduga atau diadili melakukan tindak pidana untuk melakukan kewajiban tertentu yang tidak melibatkan pidana penjara (Alicia et al. 2019).

Genoveva mengatakan, Indonesia sudah mengenal konsep alternatif pidana lewat konsep pidana denda, pidana pengawasan, pidana kerja sosial, pidana angsuran, pengembalian kepada orang tua, rehabilitas pengguna dan korban penyalahgunaan narkoba. Tetapi, alternatif pidana tidak dilakukan oleh para penegak hukum karena sejumlah alasan. Alasan paling dominan adalah tidak ada tujuan untuk menerapkan pidana alternatif sebagai hukuman (Taher 2019).

Berdasarkan penelitian ICJR, ditemukan bahwa dalam pelaksanaannya bentuk alternatif pidana ini tidak dilaksanakan dengan maksimal dan masih jauh angkanya jika dibandingkan dengan pidana penjara. Sebagai contoh, sepanjang 2016, pidana bersyarat hanya dijatuhkan pada 3.464 terpidana, di 2017 meningkat sebesar 3.909 terpidana, dan di 2018 (data hingga Oktober 2018) dijatuhkan dalam 2.252 terpidana. Jika dibandingkan,

jumlah terdakwa yang dijatuhi pidana percobaan dengan jumlah terdakwa yang dijatuhi pidana penjara hanyalah sebesar 1:5 di 2017, kemudian di tahun 2018 (data hingga Oktober) meningkat menjadi 1:8 Beberapa faktor yang diidentifikasi menjadi penyebab dari rendahnya penggunaan alternatif pidana *non-custodial* ini diantaranya yaitu (Reform 2019):

"1. Adanya perbedaan pandangan antar penegak hukum mengenai tujuan pemidanaan yang dianut. Alternatif pemidanaan non pemenjaraan
2. Lambannya perkembangan regulasi dan kebijakan mengenai alternatif pemidanaan non pemenjaraan
3. Adanya masalah dalam hal penahanan yang dijadikan sebagai "kewajiban" dalam proses peradilan pidana
4. Buruknya koordinasi antar lembaga terkait dalam pelaksanaan pidana alternatif dan minimnya kontrol
5. Kecilnya kepercayaan masyarakat dan aparat penegak hukum pada pidana alternatif dan pelaksanaannya
6. Minimnya peraturan pelaksana terkait ketentuan alternatif pemidanaan non-pemenjaraan
7. Belum tersedianya sarana dan prasarana yang memadai seperti UPT Bapas, Pembimbing Kemasyarakatan, LPAS."

Banyaknya kritik terhadap aspek-aspek negatif dari pidana penjara telah menghasilkan beberapa usaha untuk menemukan bentuk-bentuk alternatif dari pidana penjara. Sementara itu, usaha ini juga diampingi dengan adanya kecenderungan dalam praktik untuk membatasi atau menghindari penerapan pidana dan usaha untuk memperbaiki pelaksanaannya. Negara Belanda merupakan salah satu contoh negara yang telah membuktikan adanya kecenderungan menurunnya penggunaan atau penerapan pidana penjara.

Menurut Pompe, dalam praktik pengadilan di negeri Belanda terlihat suatu ketidaksukaan yang semakin besar terhadap pidana perampasan kemerdekaan dan suatu kesukaan yang semakin besar terhadap pidana denda. Data yang dikemukakan adalah sebagai berikut: Pidana penjara yang dijatuhkan hakim pada tahun 1896 ialah lebih dari 55%, tahun 1913 lebih dari 48%, tahun 1936 lebih dari 45% dan pada tahun 1955 hanya mendekati 33%, sedangkan untuk pidana denda pada tahun 1896 ialah lebih dari 30%, tahun 1913 lebih dari 40%, tahun 1936 lebih 42% dan pada tahun 1955 lebih dari 63%. Usaha untuk menghindari atau membatasi penerapan pidana penjara terlihat pula misalnya di inggris dengan adanya the *First Offenders Act* 1958 yang melarang pengadilan untuk menjatuhan pidana penjara kepada para pelaku pertama (*first offenders*), kecuali tidak ada cara lain yang dianggap tepat untuk memperlakukan mereka (Randa Ananda Lakenda 2017).

Adapun usaha untuk memperbaiki pelaksanaan pidana penjara ialah dengan adanya *Standard Minimum Rules* (selanjutnya disingkat SMR) yang semula dirancang oleh *The International Penal and Penitentiary Commision* (IPPC) pada tahun 1933. Setelah naskah IPPC ini diperbaiki oleh Sekretariat PBB, akhirnya SMR ini disetujui oleh Kongres PBB pertama mengenai Pencegahan Kejahatan dan Pembinaan Pelanggar Hukum pada tahun 1955 di Geneva. Selajutnya SMR ini disetujui oleh Dewan Ekonomi dan Sosial PBB dalam resolusimya No.663 C (XXIV) tertanggal 31 Juli 1957. Erat kaitannya dengan diterimanya SMR ini, maka kongres kedua PBB mengenai Pencegahan Kejahatan dan Pembinaan Pelanggar Hukum pada tahun 1960 di London telah mengeluarkan rekomendasi untuk membatasi atau mengurangi penggunaan yang luas dari pidana penjara khususnya pidana penjara jangka pendek. Resolusi ini jelas berkaitan erat dengan tujuan untuk menunjang pelaksanaan SMR. Untuk dapat menampung, mengawasi, dan membina para narapidana tidak boleh melampaui kapasitas lembaga yang pada umumnya disebabkan oleh besarnya jumlah narapidana yang dijatuhi pidana penjara jangka pendek (Randa Ananda Lakenda 2017).

Berbagai negara telah menyediakan dan telah menerapkan hukuman *non-custodial,* yaitu Perancis merupakan negara pertama yang memasukkan bentuk hukuman *non-custodial* berupa *probation* dalam rancangan undang-undang tahun 1884, yang kemudian diundangkan pada tahun 1891. Rancangan undang-undang ini menekankan pentingnya menghindari dampak pidana penjara jangka pendek untuk pertama kalinya. Belgia pada tahun 1888 mengadopsi kebijakan serupa, dengan syarat yang lebih ketat, yaitu hanya boleh ada alternatif hukuman penjara dijatuhkan kepada pelanggar pertama dan dalam hal hakim menjatuhkan hukuman kurang dari enam bulan. Munculnya *probation* dengan pengenalannya di Perancis kemudian berkembang di berbagai forum internasional. Sejumlah negara Eropa mulai mengadopsi ketentuan *probationary punishment* (pelaksanaan hukuman bersyarat) dengan berbagai modifikasi, antara lain Luxembourg (1892), Portugal (1893), Norwegia (1894), Italia (1904), Bulgaria (1904), Denmark (1905), Swedia (1906), Spanyol (1908), Hungaria (1908), Yunani (1911), Belanda (1915), dan Finlandia (1918). Penggunaan hukuman *non-custodial* kemudian mendapat pembenaran praktisnya. Pada tahun 1970-an, Amerika Serikat dan Inggris, dua negara yang mengalami masalah *overcrowding* yang parah, mengadopsi konsep hukuman *non-custodial*. Kedua negara ini kemudian mengembangkan berbagai jenis

hukuman *non-custodial* dengan tujuan untuk mengurangi penggunaan penjara (Alicia et al. 2019).

Berdasarkan beberapa hal di atas, kebijakan pemberian pidana perampasan kemerdekaan (penjara) tentu sudah tidak sejalan dengan perkembangan dunia pada saat ini. Maka dari itu harus diberikan kebijakan terkait perkambangan jenis-jenis sanksi pidana yang bersifat sanksi selain pidana penjara. Dalam konteks tindak pidana peretasan, kententuan pidana beberapa negara yang mengatur pidana selain penjara dalam aturan tindak pidana peretasan, yaitu sebagai berikut:

1. Belanda

Belanda sebagai bagian dari hukum Eropa Kontinental yang menerapkan sistem kodifikasi, membuat suatu ketentuan pidana dalam bentuk Kitab Undang-Undang Hukum Pidana (*Wetboek van Strafrecht*). Ketentuan mengenai tindak pidana peretasan diatur dalam Pasal 138ab Sr, yang berisi:

"*1. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:*

a. door het doorbreken van een beveiliging,

b. door een technische ingreep,

c. met behulp van valse signalen of een valse sleutel, of

d. door het aannemen van een valse hoedanigheid.

2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens

a. met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;

b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

Terjemahan:

"1. Barangsiapa dengan sengaja dan melawan hukum memasuki suatu sistem komputer atau bagiannya, diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak kategori keempat, karena melakukan penyusupan komputer. Dalam hal apa pun ada intrusi jika akses ke sistem diperoleh:

a. dengan melanggar keamanan,

b. dengan intervensi teknis,

c. menggunakan sinyal palsu atau kata sandi palsu, atau

d. dengan identitas palsu.

2. Penyusupan komputer diancam dengan pidana penjara paling lama empat tahun atau pidana denda paling banyak Kategori IV, jika pelaku kemudian mengambil alih, menyadap atau merekam data yang telah disimpan, diproses atau dipindahkan dengan cara kerja otomatis di mana dia berada secara melawan hukum, untuk dirinya sendiri atau untuk orang lain.

3. Penyusupan komputer yang dilakukan melalui perantaraan infrastruktur telekomunikasi diancam dengan pidana penjara paling lama empat tahun atau denda paling banyak Kategori IV, jika pelakunya kemudian

a. menggunakan data-data secara illegal yang diambil dari sistem terkomputerisasi milik pihak ketiga dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum;

b. memperoleh akses ke pekerjaan otomatis pihak ketiga melalui perantara pekerjaan otomatis yang telah ditembusnya."

Berdasarkan isi dari Pasal 138ab Sr di atas, terdapat 2 jenis saknsi pidana yang diancamkan bagi pelaku tindak pidana peretasan di Belanda yaitu pidana penjara dan pidana denda yang dirumuskan secara alternatif. Namun, pada tahun 2019, Polisi dan Kejaksaan Belanda telah mengembangkan intervensi *Hack_Right* sebagai prosedur alternatif pidana atau tambahan untuk pelanggar kejahatan komputer remaja. Peretas berusia antara 12 hingga 23 tahun yang telah melakukan kejahatan dunia maya untuk pertama kalinya diberi kesempatan untuk memperbaiki perilaku mereka di dalam *Hack_Right*. Anak-anak mendapat hukuman alternatif atau tambahan yang ditujukan untuk pemulihan, pelatihan dan pembinaan. *Hack_Right* bertujuan untuk mencegah residivisme di antara peserta dan menyediakan kerangka kerja di mana peserta dapat mengembangkan bakat TI mereka secara legal. Untuk mencapai tujuan ini, peserta ditautkan ke perusahaan (keamanan siber). Pada perusahaan-perusahaan ini, anak-anak muda menyelesaikan tugas di mana mereka merenungkan kejahatan mereka, belajar tentang peretasan etis (HSD Foundation 2019).

2. Uzbekistan

Uzbekistan mengadopsi aturan khusus untuk menjamin keamanan informasi yang tercantum dalam

KUHP Republik Uzbekistan Bagian VI/Bab XX-1 Kejahatan di bidang teknologi informasi. (Octopus Cybercrime Community 2020) Tindak pidana peretasan diatur dalam Pasal 174 KUHP Uzbekistan, yaitu:

"*Article 174. Computer-related Crime*

Computer-related crime, that is unauthorized access to information networks or authorized access to information networks without taking required security measures, or illegal retrieval of information therefrom, as well as intended change, loss, removal, or erasure of information during authorized work in an information system, which have resulted in a large damage – shall be punished with fine up to seventy-five minimum monthly wages, or correctional labor up to three years.

Making of computer viruses or software programs and their dissemination without due authorization with the purpose of changing data or software programs, which are stored in computer systems, as well as unauthorized access to an information system which has resulted in corruption, removal, or erasure of information, or cessation of the operation of this system –shall be punished with fine from seventy-five to two hundred minimum monthly wages, or arrest from three to six months and deprivation of certain right. (As amended by Law of 29.08.2001.)"

Terjemahan:

"Kejahatan yang behubungan dengan komputer, yaitu akses tidak sah ke jaringan informasi atau akses secara sah ke jaringan informasi tanpa melakukan tindakan pencegahan keamanan, atau pengambilan informasi secara ilegal darinya, serta memiliki tujuan melakukan perubahan, penghilangan, penghapusan, atau penghapusan informasi selama melakukan akses secara sah pada suatu sistem informasi yang mengakibatkan kerusakan besar. Dipidana dengan pidana denda paling banyak tujuh puluh lima upah bulanan, atau kerja sosial hingga tiga tahun.

Pembuatan virus komputer atau program perangkat lunak dan menyebarkannya tanpa kewenangan dengan tujuan mengubah data atau program dalam perangkat lunak yang disimpan dalam sistem komputer, serta akses tanpa hak terhadap sistem informasi yang mengakibatkan data rusak, penghilangan, atau penghapusan informasi, atau penghentian pengoperasian sistem ini akan dihukum dengan denda dari tujuh puluh lima sampai dua ratus minimum gaji bulanan, atau kurungan tiga sampai enam bulan atau perampasan hak-hak tertentu. (Amandemen dari Undang-Undang 29.08.2001)"

Berdasarkan ketentuan Pasal 174 KUHP Uzbekistan, jenis sanksi yang diancamkan kepada pelaku tindak pidana peretasan di Uzbekistan yaitu pidana denda, pidana kerja sosial, pidana kurungan dan perampasan hak-hak tertentu yang dirumuskan secara alternatif.

Di Indonesia, RKUHP *draft final* 6 Desember 2022 membagi jenis-jenis sanksi pidana dalam 3 kategori, yaitu pidana pokok (Pasal 65), pidana tambahan (Pasal 66) dan pidana yang bersifat khusus (Pasal 67). Berikut isi dari Pasal 65, Pasal 66 dan Pasal 67 RKUHP, yaitu:

Pasal 65

"(1) Pidana pokok sebagaimana dimaksud dalam Pasal 64 huruf a terdiri atas:
a. pidana penjara;
b. pidana tutupan;
c. pidana pengawasan;
d. pidana denda; dan
e. pidana kerja sosial.

(2) Urutan pidana sebagaimana dimaksud pada ayat (1) menentukan berat atau ringannya pidana."

Pasal 66

"(1)Pidana tambahan sebagaimana dimaksud dalam Pasal 64 huruf b terdiri atas:
a. pencabutan hak tertentu;
b. perampasan Barang tertentu dan/atau tagihan;
c. pengumuman putusan hakim;
d. pembayaran ganti rugi;
e. pencabutan izin tertentu; dan
f. pemenuhan kewajiban adat setempat.

(2) Pidana tambahan sebagaimana dimaksud pada ayat (1) dapat dikenakan dalam hal penjatuhan pidana pokok saja tidak cukup untuk mencapai tujuan pemidanaan.

(3) Pidana tambahan sebagaimana dimaksud pada ayat (1) dapat dijatuhkan 1 (satu) jenis atau lebih.

(4) Pidana tambahan untuk percobaan dan pembantuan sama dengan pidana tambahan untuk Tindak Pidananya.

(5) Pidana tambahan bagi anggota Tentara Nasional Indonesia yang melakukan Tindak Pidana dalam perkara koneksitas dikenakan sesuai dengan ketentuan peraturan perundang-undangan bagi Tentara Nasional Indonesia."

Pasal 67

"Pidana yang bersifat khusus sebagaimana dimaksud dalam Pasal 64 huruf c merupakan pidana mati yang selalu diancamkan secara alternatif."

Berdasarkan hal tersebut, terdapat tiga jenis alternatif pidana penjara yang ditetapkan sebagai pidana pokok, yaitu pidana pengawasan, pidana denda, dan pidana kerja sosial. Meskipun memenuhi syarat sebagai pidana pokok, dalam penjelasan Pasal 65 ayat (1) menegaskan bahwa pidana pengawasan dan pidana kerja sosial pada dasarnya merupakan model dari pelaksanaan pidana sebagai pengganti pidana penjara. Akibatnya, alternatif untuk pidana penjara, seperti pidana pengawasan, bukanlah bentuk pidana khusus dalam perumusan suatu kejahatan. Pidana kerja dan pidana pengawasan pada hakekatnya merupakan pelaksanaan pidana (*strafmodus*) sebagai

alternatif pidana penjara. Berdasarkan hal tersebut, bentuk alternatif pidana bagi pelaku tindak pidana peretasan di Indonesia:

1) Pidana Pengawasan

Hukum positif yang berlaku di Indonesia saat ini pada dasarnya telah mengatur mengenai alternatif pidana penjara yang bersifat *non-custodial* yaitu dengan diberikannya pidana bersyarat yang telah diatur dalam Pasal 14 huruf a sampai f KUHP. Ketentuan dalam Pasal 14 huruf a KUHP secara garis besar menyebutkan, bahwa terhadap terpidana yang dijatuhi pidana penjara kurang dari 1 (satu) tahum kurungan bukan pengganti denda dan denda yang tidak dapat dibayar oleh terpidana dapat digantikan dengan pidana bersyarat. Dengan demikian terhadap pelaku tindak pidana telah ada penjatuhan pidana yang secara pasti, yang pelaksanaannya ditunda dengan pidana bersyarat, sehingga terjadi proses stigmatisasi terhadap pelaku tindak pidana melalui putusan hakim yang disampaikan dalam persidangan.

Istilah pidana pengawasan atau *probation* menurut Muladi mempunyai arti sebagai suatu sistem yang berusaha untuk mengadakan rehabilitasi terhadap seseorang yang terbukti melakukan tindak pidana, dengan cara mengembalikan ke masyarakat selama suatu periode pengawasan (Muladi and Barda Nawawi Arief 1998).

Diberlakukannya pidana pengawasan dapat mengurangi kerugian yang ditimbulkan dari pidana pencabutan kemerdekaan, terutama kerugian mengenai gangguan terhadap gangguan sosial dan kesulitan terpidana untuk menyesuaikan diri dimasyarakat. Dengan demikian konsep pidana pengawasan telah mencakup teori gabungan yang dianut oleh Indonesia dengan lebih mengutamakan perlindungan terhadap masyarakat atau korban dan pelaku tindak pidana.

Tujuan diberlakukannya pidana pengawasan adalah "*to rehabilitate the offender, protect the public and prevent the offender committing further offences*". yang artinya adalah untuk merehabilitasi pelaku, melindungi masyarakat dan mencegah pelaku melakukan tindak pidana lebih lanjut (Siswanta Slamet 2007). Menurut Muladi keuntungan diberlakukannya pidana pengawasan sebagai berikut (Muladi 1992):

"a. Akan memberkan kesempatan kepada terpidana untuk memperbaiki dirinya dimasyarakat, sepanjang kesejahteraan terpidana dalam hal ini sebagai hal yang utama dibandingkan resiko yang mungkin akan diderita oleh mayarakat, apabila terpidana dilepakan dimasyarakat. dalam hal ini yang diutamakan dari pidana pengawasan adalah kesehatan mental dari terpidana.
b. Memungkinan terpidana untuk melanjutkan kebiasaan hidupnya sehari-hari sebagai manusia, sesuai dengan nilai-nilai yang ada dalam masyarakat.
c. Mencegah terjadinya stigma yang akan diakibatkan oleh pidana perampasan kemerdekaan."

Pedoman untuk menjatuhkan pidana pengawasan akan dapat dibatasi yang dicantumkan dalam undan-undang. Menurut Muladi pembatasan untuk menentukan penjatuhan pidana pengawasan adalah dengan melihat tindak pidana yang dilakukan. Tindak pidana yang tidak dapat dikenan pidana pengawasan yaitu (Muladi 1992):

"a. Kejahatan-kejahatan kekerasan;
b. Kejahatan-kejahatan terhadap moral;
c. Kejahatan yang melibatkan penggunaan senjata yang mematikan;
d. Kejahatan yang dilakukan seseorang karena diupah oleh orang lain;
e. Kejahatan terhadap pemerintah;
f. Kejahatan yang diancam dengan pidana tertentu."

Pelaku tindak pidana yang dijatuhkan pidana pengawasan ditentukan masa pengawasan, dimana dalam tanggung masa pengawasan ini pelaku dibebani dengan persyaratan. Dalam konteks tindak pidana peretasan, pidana pengawasan dapat dikombinasikan dengan perampasan hak-hak tertentu yang berhubungan dengan tindak pidana peretasan. Pasal 73 RKUHP ayat (1) huruf b menyebutkan bahwa salah satu syarat dapat dijatuhkannya pidana pengawasan yaitu terpidana harus atau tidak melakukan perbuatan tertentu, tanpa mengurangi kemerdekaan beragama, menganut kepercayaan dan berpolitik. Maka, dalam tindak pidana peretasan, syarat terpidana untuk tidak melakukan perbuatan tertentu yaitu larangan dan pencabutan hak menggunakan komputer dan/atau sistem elektronik seperti *smartphone*, *tablet*, laptop dan perangkat elektronik lain yang dapat terhubung dengan internet. Dengan bantuan alat komputer dan/atau sistem elektronik juga mengakses alat tersebut, pelaku peretasan dapat melakukan aksinya. Maka dengan melarang dan mencabut hak untuk menggunakan komputer dan/atau sistem elektronik, pelaku peretasan tidak dapat melakukan peretasan kembali.

Pelaksanaan pengawasan terhadap pelaku tindak pidana peretasan dapat dilaksanakan sesuai dengan ketentuan Ordonasi Pelaksanaan Hukuman Bersyarat (*Uitvoeringordonnatie Voorwaardelijke Veroordeeling*) dalam S. 1926 Nr. 487, yang kemudian telah diubah dan ditambah dengan S. 1928 Nr. 445 dan S. 1939 Nr.77. Dalam Pasal 2 ayat (1) ordonasi ini memberikan ketentuan sebagai berikut (Doodoh 2013):

"Dari setiap keputusan hukuman bersyarat yang mutlak harus dilaksanakan, pejabat yang diserahi menjalankan pelaksanaan itu dengan segera memberitahuan kepada *Directeur van Justitie* (yang saat ini dapat disebut dengan Kementerian Hukum dan Hak Asasi Manusia) dengan melampirkan formulir serperti yang telah diterapkan oleh ordonasi ini dan telah dilakukan pengisiannya oleh pejabat yang bersangkutan. Apabila belum ada jangka waktu permulaan dan berakhirnya percobaan, sehingga hal itu tidak dapat dengan seketika dalam formulis yang dimaksud, maka pemberitahuan mengenai hal itu secepatnya segera diusulkan"

Ketentuan terkait pelaksanaan pidana pengawasan tentunya akan dijalankan oleh Jaksa dan Kementerian Hukum dan Hak Asasi Manusia agar terpidana *cybercrime* tetap dalam pengawasan dan merehabilitasi pelaku, melindungi masyarakat dan mencegah pelaku agar tidak melakukan tindak pidana lebih lanjut.

2) Pidana Kerja Sosial

Konsep pidana kerja sosial di merupakan bagian dari penerapan *restoratif jutice* yang bertujuan untuk memulihkan konflik pada korban juga menjujung tinggi pada hak asasi manusia dan kebutuhan untuk menghindari dampat ketidakadilan sosial serta bertujuan memulihkan pelaku secara sederhana dengan memperhatikan keadilan yang bersifat formil. Dalam rangka mencari alternatif pidana penjara (*alternative to custodial sentence*) haruslah didasarkan pada pertimbangan realistis dari masyarakat. Pidana kerja sosial (*community service order*) merupakan jenis sanksi pidana untuk generasi keempat karena adanya anggapan pidana denda kurang eferktif untuk diterapkan secara luas (Wijaya and Umara 2022). Pidana kerja sosial pada dasarnya dapat diterpkan sebagai alternaitf pidana jangka pendek dengan denda yang ringan. Salah satu negara yang dapat dijadikan contoh dalam penerapan pidana kerja sosial dalah Belanda. Di Belanda, pidana kerja sosial hanya dapat dijatuhkan sebagai suatu pidana pokok alternatif, dalam contoh diancamkan pidana badan tidak bersyarat yang diancam dengan hukuman tidak lebih dari 6 (enam) bulan atapaun pidana badan pada bagian tidak bersyarat yang di eksekusi dengan ancaman hukuman tidak lebih dari 6 (enam) bulan, maka sebagai alternatif dari pidana tersebut hakim dapat menjatuhkan pidana kerja sosial. Pekerjaan yang dapat diberikan kepada pelaku tindak pidana adalah pekerjaan yang tujuannya untuk membantu pemerintah dalam menjaga dan meningkatkan *cybersecurity*. Pidana kerja sosial bagi pelaku tindak pidana peretasan di Uzbekistan diancamkan maksimal 3 tahun. Uzbekistan tidak merumuskan pidana penjara bagi pelaku tindak pidana di Uzbekistan, hal tersebut dapat mengurangi kepadatan Lembaga pemasyarakatan akibat orientasi pidana harus berupa pidana penjara.

Pidana kerja sosial dapat dijatuhkan kepada pelaku tindak pidana peretasan dengan melihat kodisi pelaku, korban tindak pidana, rasa keadilan untuk masyarakat dan keadilan hukum. Pertimbangan yang harus diperhatikan dalam memberikan pidana kerja sosial adalah harus adanya persetujuan dari terdakwa. Terpidana yang dijatuhi hukuman pidana kerja sosial maka tidak akan mendapatkan bayaran karena sifatnya adalah pidana (*work as a penalty*), oleh karena itu maka pidana tidak diperbolehkan mengandung hal-hal yang bersifat komersil. Dalam menjatuhkan pidana kerja sosial yang harus dipertimbangkan oleh hakim adalah hal sebagai berikut (Wijaya and Umara 2022):

"a) Pengakuan dari terdakwa terkait tindak pidana yang telah dilakukan;
b) Usia layak kerja terdakwa berdasarkan peraturan perundang-undangan yang berlaku;
c) Persetujuan dari terdakwa untuk melakukan kerja sosial, setelah dijelaskan oleh hakim mengenai tujuan dari pidana sosial dan segala hal yang berhubungan dengan pidana tersebut;
d) Riwayat sosial terdakwa;
e) Perlindungan terhadap keselamatan kerja terdakwa;
f) kemampuan terdakwa untuk membayar denda."

Apabila majelis hakim sepakat untuk menjatuhkan hukum pidana dalam jangka waktu lebih dari enam bulan atau kurang dari satu tahun maka pidana kerja sosial sangat tepat dijatuhkan kepada pelaku tindak pidana peretasan. Adapun alasan karena karakteristik *cybercrime* sebagai berikut :

a) Karakteristik pelaku tindak pidana peretasan mempunyai pendidikan yang relatif tinggi, mempunyai kemampuan yang memadai dalam mengoperasikan program komputer, ulet, kreatif dan menyukai tantangan;
b) Pembinaan pidana kerja sosial juga dapat menghindari terdakwa dari stigmatisasi dan prisionisasi yang timbul dari pembinaan di LAPAS;
c) Memberikan pekerjaan terhadap pelaku tindak pidana peretasan pada instansi tertentu, memberikan peluang untuk terpidana dapat dipekerjakan pada tempat dia diberikan pembimbingan seletah selesai menjalani pidana.
d) Kemampuan pelaku tindak pidana peretasan dapat dimanfaatkan untuk pengelolaan sistem informai

yang berbasis pada komputer, mislanya pada Kementerian Telekomunikasi, Kepolisian, dan perusahaan jasa di bidang teknologi dan informasi.

Istilah "pekerjaan sosial" "pelayanan masyarakat" telah dikenal di dalam KUHP beberapa negara seperti Beylorusia, Georgia, Kazakstan, dan Azerbaizan, Denmark, Inggris, Prancis, Belanda, Latvia dan Uzbekistan. Sedangkan di Amerika negara yang menerapkan sistem pidana kerja sosial adalah Peru (Tirtana 2016).

PENUTUP

Simpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Tindak pidana peretasan di Indonesia pertama kali diatur dalam Undang-Undang No 3 tahun 1989 tentang Telekomunikasi yaitu tercantum dalam Pasal 23 dan Pasal 35. Kemudian disahkannya Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi sebagai pengganti Undang-Undang Nomor 3 tahun 1989 tentang Telekomunikasi dengan alasan yang tercantum dalam konsideran yaitu pengaruh globalisasi dan perkembangan teknologi telekomunikasi yang dangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi. Ketentuan mengenai tindak pidana peretasan dalam Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi terdapat dalam Pasal 22 *jo* Pasal 50. Hingga pada tahun 2003, Kementerian Negara Komunikasi dan Informatika mulai membahas Rancangan Undang-Undang Informasi dan Transaksi Elektronik dan akhirnya disahkan pada tanggal 28 April 2008. Ketentuan mengenai tindak pidana peretasan terdapat dalam Pasal 30 *jo* Pasal 46. Kemudian Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang masih berlaku hingga saat ini merupakan upaya preventif negara untuk mengatasi kejahatan dunia maya.
2. Sanksi pidana terhadap pelaku tindak pidana peretasan yang dirumuskan dalam Pasal 138ab Sr yaitu pidana penjara dan pidana denda. Namun, Polisi dan Kejaksaan Belanda menciptakan suatu percobaan sebagai prosedur alternatif pidana atau tambahan untuk pelanggar kejahatan komputer remaja yang disebut *Hack_Right*. Remaja dengan usia 12 hingga 23 tahun mendapat hukuman alternatif atau tambahan yang ditujukan untuk pemulihan, pelatihan dan pembinaan. *Hack_Right* bertujuan untuk mencegah residivisme di antara peserta dan menyediakan kerangka kerja di mana peserta dapat mengembangkan bakat TI mereka secara legal. Berbeda halnya dengan Uzbekistan, dalam ketentuan dalam Pasal 174 KUHP Uzbekistan, sanksi pidana bagi pelaku tindak pidana peretasan yaitu pidana denda, pidana kerja sosial, pidana kurungan dan perampasan hak-hak tertentu. Bentuk alternatif pidana bagi pelaku tindak pidana peretasan di Indonesia yaitu pidana pengawasan dan pidana kerja sosial.

Saran

Berdasarkan pembahasan yang telah ditelaah diatas, beberapa saran yang dapat dikemukakan terkait dengan penelitian ini, yaitu:

1. Seiring dengan perkembangan teknologi, potensi dan keahlian yang dimiliki peretas dalam mengakses komputer dan sistem elektronik dapat dimanfaatkan untuk membuat atau mengarahkan agar perkembangan teknologi menuju ke arah yang lebih baik dengan cara seperti mengembangkan kemampuannya dalam hal menjaga dan meningkatkan *cybersecurity* di Indonesia.
2. Hukum pidana yang harus mengikuti perkembangan zaman dan teknologi, maka perlu adanya pembahasan lebih lanjut mengenai *cybercrime* terutama tindak pidana peretasan, mengingat potensi kejahatan lainnya dapat dilakukan apabila berhasil melakukan peretasan.

DAFTAR PUSTAKA

Buku

Ali, H. Zainuddin. 2009. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Hardinanto Aris. 2019. *Akses Ilegal Dalam Perspektif Hukum Pidana*. Cetakan 1. Malang: Setara Press.

Marzuki, Peter Mahmud. 2005. *Penelitian Hukum*. Jakarta: Kencana.

Muladi. 1992. *Lembaga Pidana Bersyarat*. Bandung: Alumni.

Muladi, and Barda Nawawi Arief. 1998. *Teori-Teori Dan Kebijakan Pidana*. Bandung: Alumni.

Ramli, Ahmad M. 2006. *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*. Bandung: PT Refika Aditama.

Sitompul Josua. 2021. *Cyberspace, Cybercrimes, Cyberlaw - Tinjauan Aspek Hukum Pidana*. Cetakan pertama. Jakarta: PT. Tatanusa.

Suhariyanto, Budi. 2013. *Tindak Pidana Teknologi Informasi (Cybercrime) - Urgensi Pengaturan Dan Celah Hukumnya*. Cetakan kedua. Jakarta: PT Raja Grafindo Persada.

Suparni Niniek. 2009. *Cyberscape - Problematika & Antisipasi Pengaturannya*. edited by Tarmizi. Jakarta: Sinar Grafika.

Suseno, Sigid. 2012. *Yurisdiksi Tindak Pidana Siber*. Bandung: PT Refika Aditama.

Jurnal, Skripsi, Tesis, Artikel Ilmiah, Makalah

Alicia, Genoveva, K. S. Maya, Erasmus A. T. Napitupulu, Iftitahsari M. Eka, and Ari Pramuditya. 2019. *Alternatives to Imprisonment: Provision, Implementation, and Projection of Alternatives to Imprisonment in Indonesia*.

Doodoh, Eyreine Tirza Priska. 2013. "Kajian Terhadap Penjatuhan Pidana Bersyarat Dan Pengawasan Menurut Kitab Undang-Undang Hukum Pidana." *Lex et Societatis* I.

Randa Ananda Lakenda. 2017. "Urgensi Pidana Alternatif Dalam Pembaharuan Hukum Pidana Indonesia (Studi Terhadap Pidana Alternatif Pegganti Pidana Penjara Dalam Rangka Mewujudkan Tujuan Pemidanaan)." *Universitas Negeri Semarang*.

Siswanta Slamet. 2007. "Pidana Pengawasan Dalam Sistem Pemidanaan di Indonesia." *Universitas Diponegoro*, Semarang.

Tirtana, Endang. 2016. "Community Services as an Alternative Forms of Penalty for Children in the Renewal of Children in Indonesia Criminal System." *An International Peer-Reviewed Journal* 22.

Wijaya, Tubagus Heru Dharma, and Nanda Sahputra Umara. 2022. "Penerapan Sanksi Sosial Sebagai Alternatif Pemidanaan Terhadap Pelaku Tindak Pidana Kejahatan Siber (Cyber Crime)." *Al-Qisth Law Review* 5(2).

Peraturan Perundang-Undangan

Indonesia. 2022. Rancangan Kitab Undang-Undang Hukum Pidana

Belanda. 1881. *Wetboek van Strafrecht* (WvS)

Uzbekistan. 1994. *Criminal Code of the Republic of Uzbekistan,* (No. 2012-XII)

Indonesia. 1989. Undang-Undang No 3 tahun 1989 tentang Telekomunikasi, (LN No.11 tahun 1989, TLN No. 3391).

Indonesia. 1999. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi sebagai pengganti Undang-Undang Nomor 3 tahun 1989 tentang Telekomunikasi, (LN No.154 tahun 1999, TLN No. 3881).

Indonesia. 2008. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, (LN No. 58 tahun 2008, TLN No. 4843).

Indonesia. 2016. Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, (LN No. 251 tahun 2016, TLN No. 5952).

Majelis Umum Perserikatan Bangsa-Bangsa. 1990. *United Nations Standard Minimum Rules for Non-custodial Measures (The Tokyo Rules), (General Assembly resolution* 45/11014, December 1990).

Council of Europe in Budapest. 2001. *Convention on Cybercrime*, *Europe Treaty Series* No. 185, 23 June 2001).

Website

Erdianto, Kristian. 2018. "Alternatif Pemidanaan Pada RKUHP Dinilai Tak Jadi Solusi Kelebihan Kapasitas Lapas." *Kompas.Com*. Retrieved (https://nasional.kompas.com/read/2018/06/12/17554051/alternatif-pemidanaan-pada-rkuhp-dinilai-tak-jadi-solusi-kelebihan-kapasitas?page=all).

HSD Foundation. 2019. "Pilot: Twenty Companies Help Justice Get Young Hackers on the Right Track." *Https://Securitydelta.Nl/News/Overview/Pilot-TwentyCompanies-Help-Justice-Get-Young-Hackers-on-the-Ri ght-Track*.

Kemenkumham. n.d. "Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional."*Https://Ditjenpp.Kemenkumham.Go.Id/Index.Php?Option=com_content&view=article&id=668:Dinamika-Konvergensi-Hukum-Telematika-Dalam-Sistem-HukumNasional&catid=107&Itemid=187*.

Kusnandar, Viva Budy. 2022. "Penghuni Lapas Di Seluruh Indonesia (19/9/2022) ."*Https://Databoks.Katadata.Co.Id/Datapublish/2022/09/23/Penghuni-Lapas-Dan-Rutan-Kelebihan-Kapasitas-109-Pada-September-2022*.

Muhammad, Ridwan, and Kuswandi. 2020. "Ditjen PAS Dinilai Tak Beri Solusi Sengkarut Overcrowding Rutan Dan LP." *Jawapos.Com*. Retrieved (https://www.jawapos.com/nasional/14/07/2020/ditjen-pas-dinilai-tak-beri-solusi-sengkarut-overcrowding-rutan-dan-lp/).

Octopus Cybercrime Community. 2020. "Uzbekistan."*Https://Www.Coe.Int/En/Web/Octopus/-/Uzbekistan*.

R24. 2017. "Hacker King", Indonesia?" *Pinter Politik*. Retrieved (https://www.pinterpolitik.com/in-depth/hacker-king-indonesia).

Reform, Institute for Crminal Justice. 2019. "Mencari Solusi Penjara Penuh: Saatnya Optimalisasi Alternatif Pemidanaan Non Pemenjaraan." *Icjr.or.Id*. Retrieved June 27, 2021 (https://icjr.or.id/mencari-solusi-penjara-penuh-saatnya-optimalisasi-alternatif-pemidanaan-non-pemenjaraan/).

Surfshark. 2022. "Data Breaches Rise Globally in Q3 of 2022." *Https://Surfshark.Com/Blog/Data-Breach-Statistics-2022-Q3#:~:Text=Quick%20overview*

%20 of%20Q3%202022,Indonesia%2C%20The%20U.S.%2C%20and%20Spain.

Taher, Andrian Pratama. 2019. "ICJR: Pidana Alternatif Bisa Kurangi Kelebihan Kapasitas Penjara." *Tirto.Id*. Retrieved (https://tirto .id/icjr-pidana-alternatif-bisa-kurangi-kelebihan-kapasitas-penjara-dhVB).