Jurist-Diction
Volume 5 No. 6, November 2022

Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (*Hacking*) di Indonesia

Azzahra Mazaya Khalisah dan Putri Kirana
azzahra.mazaya.khalisah-2020@fh.unair.ac.id
Universitas Airlangga

How to cite:
Azzahra Mazaya Khalisah dan Putri Kirana, 'Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (*Hacking*) di Indonesia' (2022) Vol. 5 No. 6 Jurist-Diction.

Histori artikel:
Submit 24 Oktober 2022;
Diterima 29 November 2022;
Diterbitkan 30 November 2022.

DOI:
10.20473/jd.v5i6.40073

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract

Cybercrime is a crime related to technology or cyberspace against public or private interests. Act Number 11 of 2009 concerning Information and Electronic Transactions as amended in Act Number 19 of 2019 (hereinafter referred to as UU ITE) regulates cybercrime in 9 main articles, one of which is the crime of hacking. Further investigation with cases that emerged in the last 2 years such as Hacking WhatsApp Accounts from 8 ICW Coordinators to hacking Ganjar Pranowo's Youtube account. However, Indonesian legal norms governing cybercrimes are still limited to the UU ITE. Increasing internet accessibility in Indonesia has not been harmonized with law enforcement and even faces serious issues in society. Thus, the purpose of this paper is to analyze the preventive or repressive aspects of the criminal act of hacking, the preparation of Indonesian criminal law in dealing with cybercrimes, and the punishment of criminal acts using the normative analysis method.
Keywords: *Hacking; Cybercrime; Crime.*

Abstrak

Kejahatan Siber atau Cybercrime merupakan tindak pidana atau kejahatan yang berkaitan dengan teknologi atau cyberspace terhadap kepentingan umum maupun kepentingan pribadi. Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam Undang-Undang Nomor 19 Tahun 2019 (selanjutnya disebut sebagai UU ITE) mengatur tindak pidana cybercrime dalam 9 pasal utama, salah satunya adalah tindak pidana peretasan atau hacking. Menelisik lebih lanjut dengan adanya kasus yang muncul 2 tahun terakhir seperti Peretasan Akun Whatsapp dari 8 Koordinator ICW hingga peretasan akun Youtube Ganjar Pranowo. Akan tetapi, norma hukum Indonesia yang mengatur terkait kejahatan siber masih terbatas pada UU ITE. Peningkatan aksesibilitas internet di Indonesia belum diselaraskan dengan penegakan hukum bahkan menghadapi isu serius di masyarakat. Dengan demikian, tujuan dari penulisan ini adalah menganalisa aspek preventif ataupun represif tindak pidana peretasan, persiapan hukum pidana Indonesia dalam menangani kejahatan siber, dan pemidanaan dari tindak pidana menggunakan metode analisa normatif.
Kata Kunci: *Hacking*; Kejahatan Siber; Tindak Pidana.

Pendahuluan

Perkembangan dari kejahatan siber tidak jauh dari keberadaan internet pertama kali oleh Defense Advanced Research Projects Agency atau DARPA atau projek militer dari Amerika Serikat yang mengembangkan mekanisme sistem komputer dengan bahasa komputer untuk mentransfer informasi antara dua komputer. Kemudian, pada tahun 1969 pertama kali program atau cetusan dari DARPA berhasil dilakukan oleh Universitas of California dan Stanford University. Sedangkan, di Indonesia sendiri internet mulai ada sejak tahun 1988 diawali dengan didaftarkan UI-NETLAB sebagai protokol Internet atau IP pertama di Indonesia oleh Universitas Indonesia dan sampai sekarang internet telah berkembang. Penggunaan internet membuat kegiatan sosial ataupun non-sosial dapat dilakukan melalui perangkat digital dan tidak perlu untuk menggunakan cara konvensional, sama halnya dengan sistem kearsipan, penyimpanan, komunikasi data-data penting sekarang dapat dilakukan melalui jaringan internet dan/atau jaringan komputer. Sebagai bentuk untuk mempermudah dan efisiensi dari masyarakat untuk mengakses data mereka tanpa perlu untuk melalui proses yang susah. Perkembangan dari teknologi diikuti dengan kemajuan jaringan internet dan/atau jaringan komputer yang berakibat pada peningkatan pengguna dari internet.

Berdasarkan laporan data dari We Are Social, pada awal 2022 terdapat 204,7 juta pengguna internet di Indonesia. Sedangkan, pada tahun 2018, hanya terdapat 132,7 juta pengguna internet. Perbandingan diantara kedua waktu ini memperlihatkan adanya peningkatan jumlah internet, apabila dihitung peningkatan jumlah pengguna internet sebanyak 54,25%.[1] Hal ini disebabkan, perangkat digital telah dijadikan sebagai sarana dalam kegiatan masyarakat sehari-hari. Contohnya, penggunaan perangkat digital untuk melakukan pemesanan tiket kereta atau transportasi umum, e-wallet sebagai sarana pembayaran melalui perangkat digital, dan lain-lainnya. Di satu sisi, penggunaan perangkat digital tidak dapat dihilangkan

[1] Cindy Mutia Annur, "Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022" *Databoks Katadata* (2022) <https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022>.

dari sifat masyarakat Indonesia melakukan sosialisasi di dunia maya. Laporan dari We Are Social menunjukkan sampai dengan Januari 2022 terdapat 191 juta orang yang menjadi pengguna aktif media sosial.

Sebaliknya, pada Januari 2014 terdapat 62 juta orang yang menjadi pengguna aktif media sosial. Hal ini menunjukkan adanya peningkatan dan juga tren yang hadir di Indonesia serta ketergantungan masyarakat Indonesia terhadap perangkat digital. Apabila dihitung, maka peningkatan pengguna media sosial sebanyak 129 juta orang dari tahun 2014 sampai dengan 2022.[2] Dengan demikian, akibat yang terjadi dari peningkatan pengguna internet adalah meningkatnya potensi dan kemudahakan bagi pelaku kejahatan siber untuk melakukan serangan.

Catatan Badan Siber dan Sandi Negara (BSSN) menyebutkan pada tahun 2022 terdapat 714.170.967 serangan siber yang terjadi dengan serangan siber paling tinggi terjadi pada bulan Januari dengan total 272.962.734. Dengan serangan yang dilakukan oleh para pelaku adalah serangan web defacement atau metode peretasan yang mengubah konten website sampai dengan pencurian data, serangan malware atau peretasan sistem komputer, server, atau jaringan, serangan ransomware atau pemerasan masal akibat data atau informasi pribadi yang telah dicuri, serta serangan siber lainnya. Kemudian, data dari ASEAN Cyberthreat 2021 menyatakan Indonesia merupakan negara dengan urutan pertama yang memiliki kasus paling banyak terhadap serangan malware dengan total kasus sebanyak 1,3 juta atau setengah dari keseluruhan kasus yang ada di negara ASEAN.[3] Salah satu dari kasus yang muncul 2 tahun terakhir seperti Peretasan Akun Whatsapp dari 8 Koordinator ICW hingga peretasan akun Youtube Ganjar Pranowo

Kemajuan teknologi dan informasi berdampak besar dalam menciptakan ruang siber pada kehidupan manusia sehari-hari. Terciptanya ruang siber sejalan dengan

---

[2] Alif Karnandi, "Pengguna Internet di Indonesia Capai 205 Juta pada 2022" *Data Indonesia* (8 April 2022) <https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia-capai-205-juta-pada-2022>.

[3] CNN Indonesia, "RI Dihantam 700 Juta Serangan Siber di 2022 Modus Pemerasan Dominan" *CNN Indonesia* (1 Juli 2022) <https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan>.

munculnya jenis tindak pidana yang mengancam masyarakat, serangan siber yang terjadi di Indonesia sebagaimana telah disebutkan sebelumnya merupakan salah satu tindak pidana yang mengancam masyarakat secara harta kekayaan, nyawa, kehormatan, dan/atau kemerdekaan peribadi. Secara umum, masyarakat Indonesia telah mengenal keberadaan Kitab Undang-Undang Hukum Pidana (KUHP) sebagai landasan aturan tindak pidana yang berlaku di Indonesia. Namun, eksistensi norma hukum yang mengakomodasi keberadaan informasi dan teknologi yang kini kian berkembang belum sejalan, serta masih menimbulkan kekosongan hukum. Problematika kejahatan di dunia siber mulai teratasi sejak diturunkannya ketentuan dalam UU Nomor 11 Tahun 2008 sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (atau selanjutnya disebut sebagai UU ITE). Dengan demikian, lahirnya bidang hukum baru yang kerap disebut hukum siber atau *cyber law*.

Hukum Siber (*Cyber Law*) adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara.[4] Secara umum, praktisi hukum menyebut tindak pidana yang terjadi dalam lingkup hukum siber sebagai kejahatan siber atau *cybercrime*. Definisi kejahatan siber menurut MajidYar, kejahatan siber merupakan suatu perbuatan yang tidak mengacu kepada satu jenis kejahatan melainkan beberapa jenis kejahatan ilegal dan terlarang yang memiliki kesamaan yaitu dilakukan di jaringan elektronik atau dunia maya (cyberspace).[5] Selanjutnya, MajidYar juga menjelaskan terkait lingkup dari kejahatan siber adalah jaringan elektronik, jaringan komputer, dan/atau dunia maya atau *cyberspace*. Kejahatan siber dibedakan ke beberapa jenis berdasarkan sistem pembagian David Wall's yaitu:

- *Cybertreepass*
- *Cyberpornography*
- *Cyberviolence*
- *Cyberdeception*[6]

[4] Ibrahim Fikma Edrisy, *Pengantar Hukum Siber* (Sai Wawai Publishing 2019).
[5] Roderick S Graham dan Shawn K. Smith, *Cybercrime and Digital Deviance* (Routledge 2019).
[6] *ibid.*

Penggunaan istilah "hukum siber" ini berlandaskan alasan bahwa ruang siber identik dengan sebutan dunia maya. Oxford Dictionaries memberikan definisi terkait *cyberspace,*jaringan internet dianggap sebagai ruang imajiner tanpa adanya lokasi atau tempat secara fisik denganmana komunikasi dilakukan melalui jaringan komputer. Hal ini bersesuaian dengan pendapat dari praktisi hukum di Indonesia dalam menginterpretasikan "maya" sebagai sesuatu yang semu dan tidak terlihat dalam proses pembuktian suatu tindak pidana.[7]

Dalam kejahatan siber menggunakan jaringan komputer denganmana didalamnya terdapat lingkup yang berlapis-lapis. Dalam kejahatan siber sebagaimana dalam definisi yang sudah dijelaskan sebelumnya dilaksanakan di dalam *cyberspace* yang menggunakan jaringan internet melalui jaringan komputer. Dalam hal ini, terdapat sistem berlapis antara jaringan internet dan jaringan komputer berdasarkan sistem berlapis TCP/IP sebagai berikut:

- Aplikasi (*Application*) atau program komputer atau perangkat lunak yang didesain untuk mengerjakan tugas tertentu. Selanjutnya, aplikasi bertanggung jawab untuk melakukan standarisasi data dari berbagai sumber yang ditemukan dan menyediakan *a user interface* (pemberian informasi kepada pengguna jaringan komputer atau menerima instruksi dari pengguna jaringan komputer).
- Transportasi (*Transport*) atau perpindahan dari satu tempat ke tempat yang lain dalam sebuah jaringan komputer dan/atau jaringan internet. Transportasi bertanggung jawab untuk melakukan verifikasi data dan pertukaran data antara titik akhir tertentu dalam sebuah jaringan komputer dan/atau jaringan internet. Dalam lapisan ini bertujuan untuk mengontrol hubungan atau koneksi secara langsung antara 2 atau lebih pengguna jaringan komputer dan/atau internet, sehingga lapisan ini sering disebut sebagai "*host to host*". Protokol atau seperangkat aturan yang mengontrol cara data dikirim antar jaringan komputer yang digunakan dalam lapisan ini adalah *Transmission Control Protocol* atau TCP.
- Lapisan Jaringan (*Network Layer*) atau sekelompok komputer dan perangkat yang dihubungkan dengan komunikasi sehingga informasi atau kebutuhan dapat digunakan bersama. Lapisan jaringan bertanggung jawab untuk melakukan pertukaran data di seluruh jaringan sehingga sering disebut sebagai lapisan Internet. Selain itu, dalam lapisan ini sering digunakan penyebutan *Internet Protocol* atau IP.
- Tautan (*Link*) bertanggung jawab untuk mengangkut data dari satu jaringan ke jaringan yang lain.[8]

---

[7] Ahmad M Ramli, *Cyber law & HAKI dalam sistem hukum Indonesia* (Refika Aditama 2004) <https://books.google.co.id/books?id=pqVRAgAACAAJ>.

[8] Graham dan Smith (n 5).

Selain sistem berlapis antara jaringan internet dan jaringan komputer, terdapat sistem lapisan dalam *cyberspace* berdasarkan pemikiran para ahli sebagai berikut:

- Manusia sebagai penghubungan atau yang menghubungkan komunikasi antara pengguna jaringan;
- Konten atau lapisan yang berisi informasi yang dibuat atau dibagikan dalam jaringan internet;
- Aplikasi atau program yang memperbolehkan pengguna jaringan untuk menggunakan sistem operasional dari sebuah komputer;
- Sistem Operasional atau perangkat lunak yang mengelola operasional atau penggunaan aplikasi dalam sebuah komputer;
- *Hardware* atau alat yang menghitung dan memanipulasi data
- Infrastruktur atau perangkat teknologi yang menjadi penghubung data antara dua atau lebih mesin.[9]

Dengan demikian, lapisan-lapisan yang terdapat dalam *cyberspace* berpengaruh terhadap penggolongan atau tindak pidana yang terjadi di dunia maya.

Tahapan dalam Tindak Pidana Peretasan atau *Hacking*

Peretasan atau menurut berdasarkan sistem pembagian David Wall disebut sebagai "*cybertrespass*". David Wall berpendapat, peretasan merupakan tindakan untuk berpindah dari satu tempat ke tempat yang lain tanpa persetujuan yang sah atau dalam lapisan sistem operasional jaringan komputer, serta sudah terdapat hak milik atau kepemilikan.[10] Sehingga apabila disederhanakan maka seseorang yang melakukan atau mendapatkan akses tanpa persetujuan yang resmi dianggap telah melakukan tindak pidana. Langkah-langkah dari pelaku untuk melakukan tindak pidana peretasan atau hacking dibagi 2 tahap yaitu:

1. Mendapatkan akses tanpa persetujuan resmi.

   Peretasan komputer atau sistem elektronik dapat terjadi disebabkan terjadi lemahnya atau serangan yang menyebabkan sistem operasional dan/atau perangkat lunak melemah. Lemahnya sistem operasional dan/atau perangkat lunak ini menyebabkan para pelaku mendapatkan akses tanpa persetujuan yang resmi.

[9] *ibid*.
[10] David Wall, *Crime and the Internet* (1st Editio, Routledge 2001).

- Virus atau malware yang dapat menginfeksi komputer dan mengubah serta merusak fungsi dari komputer sehingga dapat menyebabkan perangkat lunak tidak dapat berjalan sebagaimana mestinya. Penggunaan dari virus harus diaktifkan oleh pengguna komputer atau pelaku untuk mengeksekusi atau merusak fungsi dari komputer;[11]
- *Worms* merupakan malware yang dapat melakukan tindak menginfeksi komputer dan mengubah serta merusak fungsi dari komputer dengan sendirinya. *Worms* berbeda dengan virus yang harus diaktifkan oleh pengguna komputer, *worms* tidak perlu ada campur tangan dari pengguna komputer untuk mengaktifkan fungsinya karena sudah secara otomatis berjalan untuk menginfeksi fungsi dari komputer. Selain itu, untuk memasukkan *worms* ke dalam sistem komputer dapat melalui email atau tautan (*hyperlink*);[12]
- Trojans atau perangkat lunak (*software*) yang resmi. Sistem kerja dari menggunakan trojan cukup dengan pelaku mengklik trojans yang telah terinstal di sistem atau jaringan komputer kemudian pelaku dapat mengakses jaringan komputer orang lain tanpa terdeteksi. Trojan sendiri digunakan untuk membuat akses dari belakang atau akses yang tidak diketahui oleh pengguna komputer untuk mengontrol komputer milik orang lain, mengontrol pengguna komputer untuk serangan, menginstall "*keylogger*" ke komputer orang lain untuk mengetahui atau merekam kata sandi yang digunakan oleh pengguna komputer.[13]

2. Melakukan kejahatan setelah mendapatkan akses tanpa persetujuan resmi.

Setelah mendapatkan akses tanpa persetujuan resmi, selanjutnya pelaku melakukan kejahatan. Objek dari kejahatan tindak pidana peretasan atau *hacking* yang dilakukan pelaku adalah data dan/atau komputer. Sehingga, dalam tindak pidana peretasan sering kali terjadi pencurian data, manipulasi data, ataupun sabotase data.[14]

---

[11] Graham dan Smith (n 5).
[12] *ibid.*
[13] *ibid.*
[14] *ibid.*

Dengan demikian, menurut Roderick, S. Graham, seseorang dikatakan melakukan tindak pidana peretasan atau *hacking* setelah telah melakukan tindak pidana peretasan apabila setelah mendapatkan akses tanpa persetujuan resmi, pelaku melakukan kejahatan.

Norma Hukum terkait Tindak Pidana Peretasan di Indonesia

Dalam penulisan ini, pembahasan kejahatan siber hanya mencangkup terhadap tindak pidana peretasan atau *cybertrespass*. Norma hukum yang mengatur terkait tindak pidana peretasan diatur dalam UU ITE sebagai sumber hukum dalam hukum siber. UU ITE mengatur tindak pidana peretasan sebagai norma larangan dengan ketentuan pidana dalam Pasal 30 sampai dengan Pasal 32. Secara umum, UU ITE telah mengatur pelarangan tindak pidana peretasan sekaligus membagi tindak pidana peretasan dalam beberapa pasal yang berbunyi sebagai berikut:

Pasal 30 UU ITE,

(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.[15]

Pasal 31 UU ITE,

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau

[15] *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 1016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.[16]

Pasal 32 UU ITE,

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

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.[17]

Berdasarkan ketiga pasal tersebut, terdapat kesamaan unsur yaitu unsur kesalahan, unsur pelaku yang mengakses tanpa adanya persetujuan resmi, serta unsur objek dari masing-masing pasal.

Unsur "Dengan sengaja dan tanpa hak atau melawan hukum". Unsur subyektif yang memperhatikan adanya kesalahan dalam hal ini kesengajaan dan kesadaran pelaku dalam melakukan suatu tindakan yang dirumuskan sebagai larangan dalam hukum positif yang berlaku di Indonesia. Adapun maksud kesengajaan dalam pasal ini adalah dilakukan dengan kesadaran penuh dan kesengajaan apabila tindakan tersebut melawan hukum formil. Perihal tanpa hak, hakim dalam kasus yang diputus dalam Putusan No. 45/Pid.B/2012/PN.MSH menjelaskan bahwa yang

[16] *ibid.*
[17] *ibid.*

dimaksud dengan "tanpa hak" ialah tidak mempunyai hak atau izin dari pihak yang berwenang. Melawan hukum diartikan secara berbeda-beda, salah satunya oleh hoge raad yang menggunakan istilah *Zonder Eigenrecht* (tanpa hak).

Unsur "Pelaku yang mengakses tanpa adanya persetujuan resmi". Dalam UU ITE, diberikan penjelasan mengenai yang dimaksud sebagai akses. Akses merupakan kegiatan yang berinteraksi dengan sistem elektronik yang beridir sendiri atau dalam jaringan. Sedangkan, sistem elektronik merupakan perangkat dan prosedur elektronik yang digunakan dalam aspek informasi elektronik. Sehingga, yang dimaksud dengan kegiatan mengakses diantaranya adalah memiliki interaksi atau hubungan dalam suatu sistem atau jaringan elektronik yang dapat dipergunakan untuk menampilkan, mengumpulkan, menyimpan, hingga menyebarkan informasi. Sebagaimana telah dijelaskan sebelumnya bahwa tindak pidana peretasan terbagi menjadi dua tahapan yaitu, mendapatkan akses tanpa persetujuan resmi dan pelaku melakukan kejahatan. Oleh karena itu, dalam UU ITE mengatur secara spesifik terkait objek dari kejahatan yang dilakukan oleh pelaku di masing-masing pasal, sebagai berikut:

- Pasal 30 ayat (1), dalam ayat ini tidak diberikan secara spesifik terkait objek dari kejahatan. Sehingga, apabila pelaku telah mengakses komputer atau sistem elektronik tanpa persetujuan yang resmi atau *unauthorized access*, maka pelaku telah melanggar ketentuan pasal 30 ayat (1).
- Pasal 30 ayat (2), berbeda dengan pasal 30 ayat (1), pada Pasal 30 ayat (2) perancangan undang-undang memberikan objek apa yang melanggar pasal ini yaitu informasi elektronik dan/atau dokumen elektronik. Tindak pidana peretasan termasuk dalam pelanggaran pasal ini dapat berupa *data theft* atau pencurian data dan *data manipulation* atau manipulasi data. Selain itu, UU ITE memberikan penjelasan bahwa perbuatan yang dilarang dalam pasal ini adalah melakukan komunikasi, mengirimkan, memancarkan atau sengaja mewujudkan hal-hal tersebut kepada siapapun yang tidak berhak untuk menerimanya; atau sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintahan dan/atau pemerintahan daerah.
- Pasal 30 ayat (3), dalam ayat ini tidak disebutkan objek dari kejahatan. Akan tetapi, ayat ini mengatur secara khusus terkait lapisan yang harus diakses oleh pelaku yaitu salah satu lapisan yang terdapat sistem pengamanan. Berdasarkan UU ITE, sistem pengamanan yang dimaksud adalah sistem yang membatasi akses komputer atau melarang akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

- Pasal 31 ayat (1), dalam ayat ini tidak terdapat penulisan secara tertulis terkait "mengakses komputer dan/atau sistem elektronik". Namun, berdasarkan penjelasan dari UU ITE terkait intersepsi atau penyadapat yaitu kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi elektronik dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkable, seperti pancaran elektromagnetis atau radio frekuensi. Sehingga, bentuk akses tanpa persetujuan resmi dalam pasal ini dapat berupa sistem berlapis di antara jaringan internet dan komputer yaitu sistem berlapis TCP/IP. Objek yang diakses oleh pelaku yaitu komputer dan/atau sistem elektronik.
- Pasal 31 ayat (2), berbeda dengan ayat (1). Dalam ayat (2), objek dari kejahatan adalah transmisi Informasi Elektronik dan/atau Dokumen Elektronik. Dalam UU ITE, menjelaskan yang dimaksud dengan transmisi adalah pengiriman informasi elektronik dan/atau dokumen elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.
- Pasal 32 ayat (1), dalam ayat ini tindakan yang dilakukan didahului dengan akses masuk yang kemudian memenuhi unsur "mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan". UU ITE menetapkan objek kejahatan yang masuk dalam lingkup ayat ini di antaranya yaitu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik, perihal kepemilikan pihak lain ini dimaknai sebagai tindakan ilegal yang dilakukan oleh pelaku.
- Pasal 32 ayat (2), berbeda dengan ayat sebelumnya. Dalam ayat ini menggunakan unsur "memindahkan atau mentransfer" yang maksudnya menempatkan atau membawa atau memindahkan ke tempat lain. Dengan objek kejahatan yang dibedakan pada unsur "kepada Sistem Elektronik orang lain yang tidak berhak" yang maksudnya menjadikan atau memberikan akses kepada orang lain tanpa seizin pemilik untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik dalam kekuasaannya.
- Pasal 32 ayat (3), memperjelas ketentuan pada ayat (1) dengan akibat terbukanya akses terhadap suatu Informasi dan/atau Dokumen Elektronik kepada khalayak ramai dengan keutuhan data yang dapat dimanipulasi oleh pihak lain. Hal ini dapat menimbulkan tersebarnya data yang sifatnya rahasia dengan validitas yang diragukan.

Dengan demikian, tindak pidana peretasan dalam UU ITE dalam tiga pasal yaitu Pasal 30, Pasal 31, dan Pasal 32. Pasal 30 ayat (2) dan Pasal 30 ayat (3) UU ITE merupakan *lex specialis* dari Pasal 30 ayat (1).[18] Sedangkan, Pasal 31 dan Pasal 32 UU ITE merupakan bentuk lain dari Pasal 30. Pelaku mengakses tanpa persetujuan resmi, tetapi kejahatan merupakan penjabaran lebih lanjut dari

[18] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Refika Aditama 2012).

Alat Bukti Elektronik sebagai bentuk pembuktian dalam Tindak Pidana Peretasan (*Hacking*)

Implementasi UU ITE mengatur mengenai pembuktian tindak pidana siber yang prosesnya berbeda dengan tindak pidana konvensional. Materi yang termuat dalam UU ITE menyadur prinsip yang terkandung dalam beberapa peraturan hukum internasional, diantaranya adalah *Convention on Cybercrime, UNCITRAL Model Law on Electronic Commerce,* dan *UNCITRAL Model Law on Electronic Signature.*[19] Salah satu yang mendasarinya yakni asas perlindungan atau yang dikenal juga dengan asas nasional pasif, asas ini terdapat juga dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang menentukan eksistensi ancaman hukuman suatu tindak pidana di wilayah negara berlaku bagi perbuatan-perbuatan yang dilakukan di luar negeri, jika perbuatan tersebut melanggar kepentingan negara yang bersangkutan. Melalui keberadaan prinsip perlindungan setiap negara memiliki kewenangan untuk memberlakukan yurisdiksi negaranya terhadap tindak pidana yang menyangkut keamanan dan integritas atau kepentingan ekonomi yang vital.[20] Prinsip perlindungan pada UU ITE sendiri terletak pada Pasal 2 yang dirumuskan bahwa peraturan perundangan ini berlaku untuk orang yang melakukan perbuatan hukum baik berada atau di luar Indonesia yang memiliki akibat hukum di Indonesia maupun luar negeri dan merugikan Indonesia. Hal ini juga bersinggungan tentunya perihal *locus delicti* tindak pidana siber, dimana dunia siber ini *borderless* dan dikhawatirkan akan terjadi *overlapping claim*.

Sehubungan dengan definisi dari tindak pidana peretasan terdapat di ruang maya atau *cyberspace,* maka dalam persidangan agenda pembukti alat bukti yang dihadirkan oleh masing-masing mendekati dengan alat bukti elektronik. Pasal 5 UU ITE menyebutkan yang dimaksud sebagai alat bukti elektronik dapat berupa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya. Bentuk alat bukti yang digunakan ini memerlukan keahlian khusus dalam kecanggihan jaringan

[19] Edrisy (n 4).

[20] J. Starke dan Bambang Iriana Djajaatmadja, *Pengantar Hukum Internasional / Penerjemah Bambang Iriana Djajaatmadja* (Sinar Grafika 1992).

sistem yang bersifat seperti pedang bermata dua, dimana kedua sisinya memberi akses sekaligus celah untuk memalsukan identitas atau bahkan memanipulasi data pribadi orang lain. Proses pembuktian pidana di Indonesia sesuai dengan Pasal 183 KUHAP menganut pembuktian secara negatif, yaitu unsur kesalahan pelaku harus dibuktikan dengan:[21]

1. Alat bukti dan prosedur pembuktian yang tercantum dalam undang-undang; dan
2. Keyakinan hakim atas alat bukti dan prosedur pembuktian yang diimplementasikan dalam menyelesaikan kasus tersebut.

Dalam UU ITE, penggunaan frasa "Informasi Elektronik dan/atau Dokumen Elektronik" pada Pasal 5 ayat (1) dan (2) serta Pasal 44 huruf b berseberangan dengan pengaturan dalam UUD NRI Tahun 1945 dan tidak memiliki kekuatan hukum yang mengikat masyarakat selama belum ada pemaknaan khusus pada frasa tersebut menjadi alat bukti yang akan digunakan dalam rangkaian pembuktian oleh para penegak hukum. Selain itu, frasa tersebut juga tercantum pada Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi atau selanjutnya disebut dengan UU TIPIKOR. Frasa yang tercantum dalam UU TIPIKOR ini bertentangan dengan isi UUD NRI 1945 dan kembali tidak memiliki kekuatan hukum sepanjang belum dimaknai secara khusus sebagai alat bukti. Sehingga, setelah dikeluarkan Putusan MK Nomor 20/PUU-XIV/2016 dalam mendapatkan alat bukti elektronik harus sesuai dengan Pasal 31 ayat (3) yaitu harus diambil oleh penegak hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya. Dalam hal ini, UU ITE telah memperkenalkan alat bukti yang dapat digunakan dalam Pasal 5 yaitu Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya. Selanjutnya, menyesuaikan dengan kondisi Indonesia setelah pandemi, Perma No. 4 Tahun 2020 Tentang Administrasi Dan Persidangan Perkara Pidana di Pengadilan Secara Elektronik menghadirkan ketentuan baru bahwa Dokumen Elektronik yang disampaikan harus dalam bentuk *portable document format* atau PDF dan harus melalui proses verifikasi antara

[21] Raden Subekti, *Hukum Pembuktian* (Cet 5, Pradnya Paramita 1980).

dokumen yang dibacakan dengan yang diunduh. Sehingga agar dapat dihadirkan di persidangan sebagai alat bukti yang sah, alat bukti elektronik didampingi dengan hasil laboratorium forensik yang dikeluarkan oleh lembaga yang berwenang.

Kesimpulan

Tindak pidana peretasan atau hacking dibagi melalui 2 tahapan, yaitu mendapatkan akses tanpa persetujuan resmi dan melakukan kejahatan setelah mendapatkan akses yang diperoleh. Atas kejahatan dalam upaya peretasan, UU ITE mengatur ketentuan serta unsur yang mengkategorikan suatu tindakan tergolong tindak pidana peretasan. Dengan berbagai perbedaan unsur di setiap ayat pada pasalnya, memperinci pula norma hukum yang berlaku secara positif di masyarakat Indonesia. Demikian pula dengan pengaturan pembuktian tindak pidana siber dalam UU ITE yang pada prinsipnya didasari dengan asas perlindungan, asas yang eksistensinya telah dikenal melalui KUHP sebagai dasar setiap negara memberlakukan yurisdiksinya. Dalam tindak pidana peretasan, pembuktian tidak akan jauh dari alat bukti elektronik mengingat eksistensi dari kejahatan tersebut dilakukan di *cyberspace*. Sehingga, agar alat bukti tersebut memiliki kekuatan hukum maka harus dihadirkan dengan prosedur yang sesuai.

Daftar Bacaan

Buku

Edrisy IF, *Pengantar Hukum Siber* (Sai Wawai Publishing 2019).

Graham RS dan Smith ‘Shawn K., *Cybercrime and Digital Deviance* (Routledge 2019).

Ramli AM, *Cyber law & HAKI dalam sistem hukum Indonesia* (Refika Aditama 2004) <https://books.google.co.id/books?id=pqVRAgAACAAJ>.

Starke J. dan Djajaatmadja BI, *Pengantar Hukum Internasional / Penerjemah Bambang Iriana Djajaatmadja* (Sinar Grafika 1992).

Subekti R, *Hukum Pembuktian* (Cet 5, Pradnya Paramita 1980).

Suseno S, *Yurisdiksi Tindak Pidana Siber* (Refika Aditama 2012).

Wall D, *Crime and the Internet* (1st Editio, Routledge 2001).

Laman

Annur CM, "Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022" *Databoks Katadata* (2022) <https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022>.

Indonesia C, "RI Dihantam 700 Juta Serangan Siber di 2022 Modus Pemerasan Dominan" *CNN Indonesia* (1 Juli 2022) <https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan>.

Karnandi A, "Pengguna Internet di Indonesia Capai 205 Juta pada 2022" *Data Indonesia* (8 April 2022) <https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia-capai-205-juta-pada-2022>.

Perundang-undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 1016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

--halaman ini sengaja dibiarkan kosong--