BAB I

PENDAHULUAN

A. Latar Belakang

Peradaban dunia pada masa kini didominasi oleh kemajuan teknologi informasi dan komunikasi yang berlangsung hampir di semua bidang kehidupan. Teknologi informasi terutama melalui media elektronik saat ini tentu dapat dijadikan sebagai simbol perkembangan sistem seluruh dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi bergerak sangat cepat menuju modernisasi.

Dengan berkembang pesatnya teknologi saat ini, segala informasi yang berasal dari seluruh penjuru dunia dapat tersebar melalui jaringan internet yang dapat diakses secara bebas dan tanpa batas oleh masyarakat umum. Hal tersebut memungkinkan seluruh masyarakat dapat mengenal berbagai hal baru secara cepat hanya bermodalkan sebuah jaringan internet dan komputer.

Internet berkembang pesat sebagai sebuah kebudayaan dan keharusan bagi manusia di zaman modern, karena melalui internet berbagai aktivitas seperti berpikir, berkreasi dan bertindak dapat diekspresikan di dalamnya, kapanpun dan di manapun. Kehadiran internet telah membentuk dunia tersendiri yang dikenal dengan dunia maya (*cyberspace*) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer.

Kecenderungan masyarakat untuk menjadi *user* dalam *cyberspace* merupakan bukti bahwa internet telah membawa kemudahan-kemudahan pada

masyarakat. Bagi sebagian orang, munculnya fenomena ini telah mengubah perilaku manusia dalam berinteraksi dengan manusia lain, baik secara individual maupun secara kelompok. Kemajuan teknologi informasi terutama internet telah memberikan dampak positif bagi kemajuan kehidupan manusia. Namun, kemajuan teknologi tentunya akan berjalan bersamaan dengan munculnya perubahan-perubahan di bidang kemasyarakatan.

Tak dapat dipungkiri bahwa perkembangan di bidang teknologi khususnya internet menciptakan peluang-peluang baru munculnya kejahatan, khususnya kejahatan di dunia maya. Internet merupakan suatu sarana yang diciptakan oleh manusia yang memiliki kemungkinan sangat besar untuk dapat dikendalikan oleh manusia lain yang memiliki keahlian di bidang yang sama.

Kejahatan dengan memanfaatkan komputer saat ini merupakan suatu kejahatan yang sedang berkembang di Indonesia, yang dikenal dengan istilah kejahatan komputer (*computer crime*). Dalam suatu studi di Amerika Serikat terdapat empat kategori kejahatan komputer yaitu:[1]

1. Pemasukan data yang tidak benar (*fraudulent*);
2. Penggunaan atas fasilitas-fasilitas yang berhubungan dengan komputer;
3. Merubah atau merusak informasi atau arsip;
4. Pencurian baik secara elektronik atau dengan cara-cara lain uang, benda, fasilitas-fasilitas dan data berharga.

Perkembangan kejahatan di dunia mayantara kini juga dikenal dengan istilah kejahatan siber (*cybercrime*). Dalam beberapa kepustakaan, kejahatan

[1] Al Wisnubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya Yogyakarta, hlm. 26.

siber (*cybercrime*) sering diidentikkan sebagai *computer crime*. *Netherlands Government Website* menjelaskan:

> *Cybercrime takes many forms, and it is therefore difficult to fight. The common forms of cybercrime include: phising, misusing personal information (identity theft), hacking, spreading hate and inciting terrorism, distributing child pornography and grooming (making sexual advances to minors)*[2]

Dari penjabaran di atas kejahatan siber (*cybercrime*) meliputi kejahatan yang sudah tidak asing lagi seperti pencurian identitas, mematikan atau menyalahgunakan situs *website* atau jaringan komputer, pembajakan, menyebarkan kebencian secara *online*, pornografi dan lain-lain. Berbagai tindakan tersebut dilakukan secara khusus dengan sarana komputer dan internet.

Berdasarkan kutipan di atas, salah satu fenomena kejahatan siber (*cybercrime*) yang sedang berkembang saat ini adalah peretasan (*hacking*). Peretasan (*hacking*) merupakan sebuah kegiatan ilegal karena masuk dan membaca data seseorang dengan tanpa izin dengan cara sembunyi-sembunyi atau sama saja dengan membodohi orang[3]. Para peretas (*hacker*) selalu menyembunyikan identitas mereka.

Kasus peretasan yang pernah terjadi di Indonesia adalah peretasan terhadap situs Dewan Pers pada bulan Mei 2017. Dalam cnnindonesia.com disebutkan bahwa tim Direktorat Tindak Pidana (Dirtipid) Siber Bareskrim menangkap inisial AS alias M2404 alias pemulungelektronik@gmail.com, yang telah melakukan peretasan terhadap *website* Dewan Pers dengan *Homepage* www.dewanpers.or.id. Inisial AS ini mengubah tampilan muka web (*deface*)

[2] https://www.government.nl/topics/cybercrime/forms-of-cybercrime, 18 Maret 2018, 21:04.
[3] Maskun, 2013, *Kejahatan Siber: Cyber Crime Suatu Pengantar*, Jakarta: Prenada Media, hlm. 43.

Dewan Pers menjadi berwarna hitam. Selain itu, di halaman utamanya terdapat gambar yang mirip burung garuda dan sebuah tulisan berwarna merah yang berisi pesan mengenai kondisi Indonesia yang menurutnya tengah terpecah. Adapun pesan yang ditulis inisial AS dalam *website* milik Dewan Pers sebagai berikut[4]:

> Ketika garuda kembali terluka karena provokasi makhluk durjana. Ketika semboyan "Bhinneka Tunggal Ika" kembali terabaikan karena aksi oknum yang mengatasnamakan agama. Ketika ayat-ayat suci jadi bahan perdebatan orang-orang yang merasa memiliki surga. Ketika perjuangan pahlawan kemerdekaan sudah dilupakan begitu saja oleh mereka yang paling merasa berjasa. Tolong hentikan semua perpecahan ini tuan. Negaraku bukan satu agama atau milik kelompok perusak. Adat, budaya juga bukan milik satu golongan.
> #DamailahIndonesiaku #JayalahBangsaku #KitaIndonesia
> M2402 2017

Meskipun sekilas isi pesan yang ditulis inisial AS berisikan pesan yang dapat dinilai bernada positif serta merupakan suatu hak yang dimilikinya sebagai seorang individu mengeluarkan pendapatnya (Pasal 28E ayat 3 UUD 1945), namun cara yang digunakan oleh inisial AS tentu saja keliru karena telah dikategorikan sebagai tindakan peretasan (*hacking*). Tindakan peretasan ini tentu merupakan suatu pelanggaran terhadap Pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dan ditambah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang menyatakan bahwa: "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer*

[4] http://tekno.liputan6.com/read/3271708/situs-resmi-dewan-pers-diretas-hacker, 19 Maret 2018, 23.00.

dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun". Sanksi pidana terhadap tindak pidana peretasan ini juga telah diatur dalam Pasal 46 ayat (1) UU ITE yang berbunyi "*Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)*".

Atas tindakannya tersebut inisial AS alias M2404 didakwa dengan Pasal 48 ayat (1) jo Pasal 32 ayat (1) Undang-Undang Nomor 11 tahun 2008 sebagaimana diubah dan ditambah dengan Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Pengadilan Negeri Surakarta menjatuhkan putusan pidana penjara 1 (satu) tahun dan 3 (tiga) bulan.

Kasus AS alias M2404 hanyalah satu dari sekian kasus peretasan yang sudah diputus di tingkat pengadilan dengan memberikan sanksi pidana yang sesuai. Meskipun demikian, adanya sanksi yang telah diatur tersebut tidak dapat menghentikan para peretas (*hacker*) untuk terus melakukan aksinya. Nampaknya, sanksi yang diberikan tidak dapat memberikan rasa jera, takut maupun khawatir akan jerat hukum yang menanti apabila melakukan tindak pidana tersebut.

Telah banyak kasus tindak pidana peretasan (*hacking*) yang telah melewati tahapan penyidikan di tingkat kepolisian hingga masuk tahap putusan di tingkat Pengadilan. Namun, hal tersebut tidak menghentikan langkah peretas (*hacker*) di luar sana yang berusaha mengikuti jejak para peretas (*hacker*) lainnya yang

telah jelas mendapatkan sanksi atas tindakan ilegal yang dilakukannya. Hal ini mengindikasikan bahwa dalam hal memberikan putusan di tingkat Pengadilan terhadap pelaku tindak pidana peretasan (*hacking*) dirasa belum optimal dan belum dapat memberikan efek jera bagi pelaku, serta hukum yang diberlakukan pun belum mampu mengurangi perkembangan tindak pidana peretasan (*hacking*) di Indonesia. Beberapa alasan yang membuat Penulis meneliti hal ini adalah:

1. Kerentanan situs Dewan Pers yang mudah di *deface*.
2. Dalam pra penelitian, motif pelaku adalah sekedar coba-coba. Hal ini memberikan dorongan kepada Penulis untuk mengetahui sejauh mana motif ini berpengaruh terhadap Pertimbangan Hakim dalam menjatuhkan putusan.

Berkaitan dengan seluruh uraian di atas, maka Penulis tertarik untuk melakukan penelitian berjudul: "**Pertimbangan Hakim dalam Menjatuhkan Sanksi Pidana terhadap Pelaku Tindak Pidana Peretasan pada Putusan Nomor 399/Pid.sus/2017/PN.Skt".**

B. Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian adalah sebagai berikut:

1. Bagaimana pertimbangan Majelis Hakim dalam menjatuhkan sanksi pidana terhadap pelaku tindak pidana peretasan pada putusan nomor 399/Pid.sus/2017/PN.Skt?

2. Apa saja hambatan yang dihadapi Majelis Hakim dalam menjatuhkan sanksi pidana dalam putusan nomor 399/Pid.sus/2017/PN.Skt?

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengetahui pertimbangan Majelis Hakim dalam menjatuhkan sanksi pidana terhadap pelaku tindak pidana peretasan pada putusan nomor 399/Pid.sus/2017/PN.Skt.
2. Untuk mengetahui hambatan yang dihadapi Majelis Hakim dalam menjatuhkan sanksi pidana dalam putusan nomor 399/Pid.sus/2017/PN.Skt.

D. Manfaat Penelitian

Berdasarkan tujuan penelitian di atas, diharapkan penelitian ini akan memberikan manfaat, baik secara teoretis maupun praktis yaitu:

1. Manfaat Teoretis

   Diharapkan penelitian ini dapat bermanfaat bagi pengembangan ilmu hukum khususnya hukum pidana berkaitan dengan Pertimbangan Hakim dalam menjatuhkan sanksi pidana dalam suatu kasus khususnya kasus tindak pidana peretasan dan juga bagi perkembangan hukum siber (*cyberlaw*).

2. Manfaat Praktis

Hasil penelitian ini dapat digunakan sebagai bahan masukan kepada pemerintah dan aparat penegak hukum dalam proses penegakan kasus tindak pidana peretasan.

E. Metode Penelitian

1. Metode Pendekatan

Metode pendekatan yang akan digunakan dalam penelitian ini adalah kualitatif, yaitu pendekatan yang tidak mengedepankan angka-angka statistik melainkan mengedepankan makna dari kenyataan di lapangan yang diteliti. Metode kualitatif adalah metode dalam suatu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka, difokuskan untuk mengkaji penerapan kaedah-kaedah atau peraturan perundang-undangan dan memahaminya kemudian meninjau pada keadaan di lapangan[5].

2. Spesifikasi Penelitian

Spesifikasi penelitian ini adalah deskriptif analitis. Deskriptif maksudnya adalah Penulis akan memberikan gambaran mengenai Pertimbangan Hakim dalam menerapkan sanksi pidana terhadap pelaku tindak pidana peretasan, secara khusus dalam kasus yang diangkat dalam penelitian yakni kasus Nomor 399/Pid.sus/2017/PN.Skt di Pengadilan Negeri Surakarta. Isi putusan ini akan dikaji apakah sudah sesuai dengan konteks penegakan hukum terhadap pelaku tindak pidana peretasan.

[5] Abdulkadir Muhammad, 2004, *Hukum dan Penelitian Hukum*, Bandung: PT Citra Aditya Bakti, hlm. 14.

Analitis maksudnya Penulis menganalisis hasil yang dideskripsikan tersebut dengan peraturan perundang-undangan terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta peraturan perundang-undangan lainnya yang terkait dengan kasus tersebut.

3. Objek Penelitian

Objek penelitian ini adalah seluruh informasi yang berkaitan dengan Pertimbangan Hakim dalam menjatuhkan sanksi pidana terhadap pelaku tindak pidana peretasan. Elemen-elemen yang akan diteliti oleh Penulis dapat diuraikan sebagai berikut:

a. Putusan Pengadilan Negeri Surakarta Nomor 399.Pid.sus/2017/PN.Skt.
b. Hakim Pengadilan Negeri Surakarta.
c. Peraturan perundang-undangan yang terkait dengan kasus tindak pidana peretasan.

4. Jenis dan Teknik Pengumpulan Data

Jenis dan teknik pengumpulan data yang digunakan dalam penelitian ini antara lain:

a. Data Primer

Data ini diperoleh langsung dari lapangan penelitian sebagai data pertama yang belum diolah oleh peneliti lain, melalui

wawancara langsung kepada para pihak terkait yaitu Hakim Pengadilan Negeri Surakarta dengan *locus* wawancara dan pengumpulan data di Pengadilan Negeri Surakarta.

b. Data Sekunder

Data ini diperoleh melalui studi kepustakaan yang digunakan untuk mempelajari literatur terkait objek penelitian, pendapat para ahli, serta peraturan perundang-undangan yang terkait penelitian. Data sekunder terdiri dari:

1) Bahan hukum primer

a) Kitab Undang-Undang Hukum Pidana (KUHP);

b) Kitab Undang-Undang Hukum Acara Pidana (KUHAP);

c) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

d) Putusan Pengadilan Negeri Surakarta Nomor 399/Pid.sus/2017/PN.Skt.

2) Bahan hukum sekunder

Bahan hukum sekunder yang digunakan adalah bahan-bahan yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer. Dalam penelitian ini digunakan hasil karya

ilmiah para sarjana, laporan penelitian dan hasil pemikiran yang tertuang dalam makalah atau literatur yang berkaitan dengan penerapan sanksi pidana terhadap pelaku tindak pidana peretasan.

3) Bahan hukum tersier

Bahan yang memberikan penjelasan informasi tentang bahan hukum primer dan bahan hukum sekunder yang terdiri dari Bibliografi, Kamus Hukum, Kamus Bahasa Indonesia atau Kamus Bahasa Inggris dan Ensiklopedia yang berhubungan dan dapat memberikan penjelasan informasi terkait permasalahan yang diteliti bilamana dibutuhkan[6].

5. Teknik Pengolahan dan Penyajian Data

Sebelum melakukan analisis, seluruh data yang diperoleh akan diolah, disusun dan dipaparkan untuk memudahkan proses analisis. Data diolah dengan teknik *editing*. Setelah proses pengolah data selesai dan untuk menjawab pertanyaan penelitian, kemudian data tersebut dianalisis dan disusun secara sistematis dan disajikan dalam bentuk laporan penelitian berbentuk skripsi.

6. Metode Analisis Data

Metode analisis data yang dipakai dalam penelitian ini metode analisis kualitatif. Metode ini menguraikan data penelitian yang telah diperoleh, kemudian memberikan penjelasan yang berkualitas, utuh,

[6] *Ibid.*

sehingga mampu memberikan gambaran mengenai permasalahan yang diteliti. Analisis data ini merupakan penjelasan dari hasil-hasil penelitian yang diperoleh dan dilaporkan dalam bentuk laporan hasil penelitian yang berbentuk skripsi.

F. Sistematika Penulisan

Sistematika Penulisan yang digunakan oleh Penulis adalah sebagai berikut:

BAB I : adalah bab Pendahuluan yang berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika Penulisan.

BAB II : adalah bab Tinjauan Pustaka yang terdiri dari tinjauan tentang pertimbangan hakim, tinjauan tentang tindak pidana, tinjauan tentang pemidanaan, tinjauan tentang putusan hakim dan tinjauan tentang tindak pidana peretasan (*hacking*).

BAB III : adalah bab Pembahasan yang terdiri dari profil pengadilan negeri surakarta, pertimbangan majelis hakim dalam menjatuhkan sanksi pidana terhadap pelaku tindak pidana peretasan pada putusan nomor 399/pid.sus/2017/pn.skt dan hambatan yang dihadapi majelis hakim dalam menjatuhkan sanksi pidana dalam putusan nomor 399/pid.sus/2017/pn.skt.

BAB IV : adalah bab Penutup yang terdiri dari simpulan yang diberikan penulis dari hasil penelitian dan pembahasan serta adanya saran-saran yang sifatnya operasional.