BAB I

PENDAHULUAN

A. Latar Belakang

Teknologi telah berkembang sangat pesat. Teknologi sangat mempengaruhi kehidupan masyarakat dalam berbagai hal dari berbagai golongan. Tidak dapat dipungkiri lagi bahwa keberadaan teknologi sangat diperlukan manusia untuk melakukan sesuatu di masa sekarang ini. Teknologi sudah menjadi kebutuhan dalam kehidupan masyarakat.

Salah satu perkembangan teknologi yang sangat cepat ada di bidang informasi dan komunikasi. Teknologi informasi dan komunikasi sangat penting karena teknologi ini yang paling besar dampaknya dalam kehidupan bermasyarakat. Segala informasi yang disampaikan dan bagaimana informasi tersebut disampaikan sering kali dapat mempengaruhi kehidupan suatu masyarakat secara luas maupun global. Perkembangan teknologi ini menyebabkan terciptanya dunia tanpa batas (*borderless*) dan perubahan sosial yang terjadi dengan sangat cepat[1].

Akibat perkembangan yang cepat ini, perkembangan teknologi sulit dikontrol. Perkembangan teknologi ini dapat menuju ke hal positif maupun negatif. Teknologi dapat digunakan untuk membantu peningkatan kesejahteraan, kemajuan, serta peradaban manusia atau digunakan oleh pihak-pihak yang tidak bertanggung jawab sebagai sarana perbuatan melawan hukum. Dari perbuatan-perbuatan melawan hukum yang kemudian dilakukan, berkembanglah *cybercrime*. *Cybercrime* adalah berbagai bentuk kejahatan yang terjadi akibat penyalahgunaan teknologi internet. Beberapa sumber mengidentikkan *cybercrime* dengan *computer crime*[2]. Karena

---

[1] Ahmad M.Ramli, 2004, *Cyber Law dan HAKI dalam Sistem Hukum Di Indonesia*, Bandung, PT. Refika Aditama, hlm 1.

[2] Eliasta Ketaren, 2016, "Cyber Crime, Cyberspace, dan Cyberlaw", *Jurnal TIMES,* Vol. 5, Nomor 2, hlm. 36, diakses pada tanggal 28 September 2020 dari http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/view/556.

perkembangan *cybercrime* yang semakin tidak terkontrol dapat menyebabkan suatu pihak rentan akan *cybercrime*. Menurut data Badan Siber dan Sandi Negara (BSSN), ditemukan sebanyak 88.414.296 kasus serangan siber pada periode 1 Januari 2020 sampai dengan 12 April 2020. Dari periode tersebut, tanggal 12 Maret 2020 menjadi puncak serangan siber dengan jumlah 3.334470 serangan[3]. Usaha untuk menekan kejadian seperti inilah yang kemudian dinilai bahwa perkembangan tersebut perlu melibatkan berbagai bentuk regulasi , dan dari bentuk yang ketat seperti kontrol yang dipimpin oleh pemerintah melalui hukum pidana dan hukum acara pidana[4].

Kejahatan terkait komputer, kejahatan dunia maya, kejahatan elektronik , dan kejahatan teknologi digital adalah fenomena yang sudah lama ada. Setiap aktivitas kriminal itu melibatkan komputer baik sebagai instrumen, target, atau sarana untuk melaksanakan aktivitas kriminal tersebut lebih jauh termasuk dalam lingkup *cybercrime*[5]. Dari sekian banyak *cybercrime* dan serangan siber, kejahatan yang paling sering terjadi adalah peretasan. Peretasan (*hacking*) pada hakikatnya adalah kegiatan mencari fungsi dari suatu sistem yang tidak sesuai dan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab, yang dapat menjadi celah dalam keamanan sistem tersebut, kemudian memperbaikinya[6]. Tapi di masa sekarang ini, peretasan dilakukan sebagai kegiatan kejahatan yang dilakukan untuk mendapat keuntungan pribadi, seperti pencurian data dengan akses ilegal dan merusak suatu sistem agar tidak dapat berjalan sebagaimana mestinya. Contohnya pada akhir bulan Mei tahun 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) diretas. Akibatnya, 279 juta data penduduk Indonesia diduga bocor dan dijual di forum

[3] Badan Siber dan Sandi Negara, Online, Internet, 20 April 2020, diakses pada tanggal 3 Februari 2022 dari https://bssn.go.id/rekap-serangan-siber-januari-april-2020/.

[4] Tatiana Tropina dan Cormac Callanan, 2015, *Self- and Co- Regulation in Cyber Crime, Cybersecurity and National Security*, New York: Springer International Publishing, hlm 4, diakses pada tanggal 26 September 2020 dari https://1lib.us/book/2570362/12d059.

[5] Mohamed Chawki *et al.*, 2015, *Cyber crime, Digital Forensics and Jurisdiction*, New York: Springer International Publishing, hlm 3, diakses pada tanggal 26 September 2020 dari https://1lib.us/book/2527038/0066cc.

[6] Jon Erickson, 2008, *Hacking: The Art of Exploitation, 2nd Edition*, California: No Starch Press, hlm 5, Diakses pada tanggal 3 Februari 2022 dari https://id1lib.org/book/1053096/4eac6c.

online. Lalu pada tanggal 27 Juli 2021, perusahaan Bank Rakyat Indonesia (BRI) Life juga menjadi korban peretasan. Akibat yang terjadi sama dengan kasus BPJS sebelumnya, yaitu data 2 juta nasabah perusahaan tersebut diduga bocor dan dijual di dunia maya. Data-data yang tersebar melalui jaringan elektronik di dalam dunia maya tersebut akan digunakan untuk kepentingan di dunia nyata. Jika data tersebut disalahgunakan, dapat menyebabkan kerusakan yang besar di dunia nyata[7].

Berangkat dari fenomena ini, sejumlah kalangan menganggap perlu segera diadakannya pengaturan terhadap dunia maya serta aktivitas-aktivitas yang terjadi disana. Dasar pemikirannya adalah hukum, sebagaimana kodratnya diperlukan di dunia maya agar aktivitas-aktivitas yang terjadi di dalamnya dapat teratur dan terkontrol[8]. Untuk peraturan internasional sendiri ada *Convention on Cybercrime* (COC) yang merupakan konvensi tentang *cybercrime* yang digagas oleh Uni Eropa. Konvensi ini pertama kali diadakan oleh Majelis Eropa (*Council of Europe*), tapi pada perkembangannya konvensi ini dapat diratifikasi oleh negara-negara yang berkomitmen untuk mengatasi kejahatan *cyber*[9]. COC sendiri di Indonesia sudah direncanakan untuk diratifikasi dan sudah dibuat Rancangan Undang-Undang (RUU) tentang Pengesahan *Convention on Cybercrime* 2001 (Konvensi Uni Eropa Tentang Kejahatan Melalui Internet, 2001). Latar belakang adanya konvensi ini karena meyakini hal ini sebagai kebutuhan untuk mengikuti kebijakan pidana umum yang ditujukan sebagai prioritas untuk melindungi masyarakat dari kejahatan dunia maya, antara lain dengan mengadopsi undang-undang yang sesuai dan mendorong kerja sama internasional, dan karena khawatir dengan risiko bahwa jaringan komputer dan informasi elektronik dapat digunakan untuk melakukan tindak pidana dan bukti yang

---

[7] Danrivanto Budhijanto, 2019*, Cyberlaw & Revolusi Industri 4.0,* Bandung: LOGOZ PUBLISHING, hlm 21, diakses pada tanggal 26 September 2020 dari https://literasidigital.id/books/cyberlaw-dan-revolusi-industri-4-0/.

[8] Galuh Kartiko, 2013, "Pengaturan Terhadap Yurisdiksi *Cyber Crime* Ditinjau dari Hukum Internasional", *Jurnal Fakultas Hukum Universitas Trunojoyo Madura,* Vol. 8, nomor 2, hlm. 4, diakses pada tanggal 22 September 2020 dari https://journal.trunojoyo.ac.id/rechtidee/article/view/695.

[9] Akbar Kurnia Putra, 2014, "Harmonisasi Konvensi *Cyber Crime* dalam Hukum Nasional", *Jurnal Ilmu Hukum Jambi*, Vol. 6, Nomor 1, hlm. 96, diakses pada tanggal 22 September 2020 dari https://www.neliti.com/publications/43297/harmonisasi-konvensi-cyber-crime-dalam-hukum-nasional.

berkaitan dengan pelanggaran tersebut dapat disimpan dan ditransfer oleh jaringan tersebut.

Keberadaan *cybercrime,* termasuk peretasan menimbulkan kesulitan seperti sulitnya menentukan lokasi kejahatan tersebut dilakukan. *Cybercrime* dapat dikategorikan kejahatan transnasional jika tidak hanya bersifat lintas negara, tetapi termasuk juga kejahatan yang dilakukan oleh suatu warga negara di suatu negara, tetapi berakibat fatal bagi negara lain[10]. Sehubungan dengan kekhawatiran akan ancaman *cybercrime* yang dapat menjadi kejahatan transnasional, diperlukan penanganan-penanganan khusus. Perserikatan Bnagsa-Bangsa (PBB) dalam Kongres PBB ke-8 mengangkat *cybercrime* (pada waktu itu disebut *computerization of criminal* justice) sebagai salah satu *draft* yang dibahas dalam kongres tersebut. Dalam Kongres PBB ke-10 juga disebutkan bahwa mengembangkan ketentuan mengenai pencegahan dan kontrol terhadap *cybercrime* (pada waktu itu disebut *computer-related* crime) menjadi hal yang penting untuk menghadapi abad ke-21. Hal-hal tersebut diperlukan sebab hal tersebut menyangkut berbagai pihak dari negara-negara serta berbagai peraturan yang berbeda-beda ketentuannya. Di Indonesia sendiri pengaturan tentang *cybercrime* sendiri sudah diatur dalam Undang-undang Nomor 11 Tahun 2008 ITE, tapi bagaimana jika *cybercrime* tersebut masuk dalam kejahatan transnasional? Pengaturan seperti apa serta ketentuan apa yang berlaku untuk menangani kasus tersebut? Berdasarkan uraian diatas maka penting untuk meneliti persoalan *cybercrime* transnasional yang dilakukan pelaku dari Indonesia berdasarkan perspektif hukum Internasional maupun hukum nasional suatu negara.

B. Rumusan Masalah

1. Bagaimana ketentuan dalam *Convention on Cybercrime* terhadap *cybercrime* khususnya peretasan?

[10] Neil Boister, 2012, *An Introduction to Transnational Criminal Law,* Oxford: Oxford University Press, hlm 4, diakses pada tanggal 27 September 2020 dari https://1lib.us/book/2799471/a1b180.

2. Bagaimana penerapan ketentuan dalam *Convention on Cybercrime* terhadap kejahatan peretasan transnasional kepada pelaku Warga Negara Indonesia?

C. Tujuan Penelitian

Tujuan yang akan dicapai dengan dibuatnya penelitian ini adalah sebagai berikut:

1. Mengetahui ketentuan dalam *Convention on Cybercrime* terhadap *cybercrime* khususnya peretasan.
2. Mengetahui penerapan ketentuan dalam *Convention on Cybercrime* terhadap Warga Negara Indonesia pelaku kejahatan peretasan transnasional.

D. Manfaat Penelitian

Selain dari tujuan diatas, penelitian ini juga memberikan manfaat antara lain sebagai berikut :

1. Memberikan informasi mengenai ketentuan dalam *Convention on Cybercrime* terhadap *cybercrime* khususnya peretasan.
2. Memberikan informasi mengenai penerapan ketentuan dalam *Convention on Cybercrime* terhadap Warga Negara Indonesia pelaku kejahatan peretasan transnasional.

E. Metode Penelitian

1. Metode Pendekatan

Dalam penelitian ini digunakan metode pendekatan yuridis sosiologis. Metode pendekatan yuridis sosiologis adalah metode pendekatan yang fokus terhadap perubahan keadaan masyarakat yang disebabkan oleh penerapan suatu sistem hukum[11]. Pendekatan yuridis sosiologis ini bertujuan untuk mendapatkan pengetahuan tentang hukum secara empiris dengan menerapkan langsung ke objeknya, yaitu terhadap warga negara Indonesia pelaku kejahatan peretasan transnasional, dengan hukum yang akan diterapkan yaitu *Convention on Cybercrime.*

[11] Laurensius Arliman S., 2018, "Peranan Metodologi Penelitian Hukum Di Dalam Perkembangan Ilmu Hukum Di Indonesia", *Jurnal Soumatera Law Reviewt*, Vol. 1, Nomor 1, hlm. 122, diakses pada tanggal 8 Juni 2022 dari http://ejournal.lldikti10.id/index.php/soumlaw/article/view/3346.

2. Spesifikasi Penelitian

Spesifikasi penelitian ini yaitu deskriptif analitis, penelitian ini bersifat deskriptif karena penelitian ini bertujuan untuk memberikan gambaran secara rinci, sistematis, dan menyeluruh mengenai segala hal yang berhubungan dengan *Convention on Cybercrime*, peretasan, serta penerapan *Convention on Cybercrime* pada warga negara Indonesia pelaku *peretasan.*

3. Objek Penelitian

Objek penelitian dalam penelitian ini adalah bagaimana penerapan *Convention on Cybercrime* pada warga negara Indonesia pelaku peretasan transnasional, serta segala informasi yang berhubungan dengan *Convention on Cybercrime* dan peretasan.

4. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah :

a. Studi Lapangan

Studi lapangan yaitu penulis terjun langsung menuju ke lapangan untuk melakukan penelitian. Studi lapangan yang akan digunakan oleh penulis dalam penelitian ini yaitu wawancara. Studi lapangan dilakukan untuk memperoleh data primer. Data primer merupakan data yang diperoleh langsung dari masyarakat. Data primer yang akan digunakan adalah data mengenai *Convention on Cybercrime*, peretasan, serta penerapan *Convention on Cybercrime* pada warga negara Indonesia pelaku peretasan.

b. Studi Kepustakaan

Studi kepustakaan dilakukan oleh penulis guna mengumpulkan data sekunder. Studi kepustakaan akan dilakukan di dua tempat, yaitu Perpustakaan Unika Soegijapranata dan Perpustakaan Kota Semarang, serta akan dilakukan studi kepustakaan secara *online* melalui internet.

Data sekunder merupakan data yang diperoleh dengan melakukan studi kepustakaan. Data sekunder terdiri dari :

1) Bahan Hukum Primer

Bahan Hukum Primer merupakan bahan hukum yang terdiri dari peraturan perundang – undangan. Bahan hukum primer yang digunakan dalam penelitian ini adalah peraturan perundang – undangan yang terkait dengan *cybercrime* dan hukum internasional. Peraturan perundang – undangan tersebut adalah :

a) *Convention on Cybercrime* (Konvensi Uni Eropa Tentang Kejahatan Melalui Internet).
b) Undang-undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

2) Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan yang berhubungan erat dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer. Bahan hukum sekunder yang digunakan pada penelitian ini yaitu hasil karya ilmiah, laporan penelitian, dan hasil pemikiran yang tertuang dalam makalah.

3) Bahan Hukum Tersier

Bahan hukum tersier yang digunakan adalah bahan yang menjelaskan tentang segala yang berhubungan dengan *Convention on Cybercrime*, peretasan, serta penerapan *Convention on Cybercrime* pada warga negara Indonesia pelaku peretasan dan memberikan informasi tentang bahan-bahan hukum primer dan sekunder. Bahan hukum tersier yang digunakan dalam penelitian ini berupa Kamus Besar Bahasa Indonesia, ensiklopedia, serta indeks kumulatif.

5. Teknik Pengolahan dan Penyajian Data

Data primer dan sekunder yang diperoleh dari penelitian telah terkumpul melalui kegiatan pengumpulan data, kemudian diolah diperiksa, dipilih, dan dilakukan editing. Setelah proses pengolahan data selesai, data akan disusun secara sistematis dan disajikan dalam bentuk uraian-uraian dan nantinya akan dibuat dalam bentuk laporan penelitian, untuk menjawab pertanyaan penelitian.

6. Metode Analisa Data

Metode analisis data yang digunakan dalam penelitian ini adalah metode analisis data kualitatif. Metode analisis data kualitatif adalah metode yang fokus mendapatkan pemahaman mengenai fenomena yang diteliti[12]. Metode ini digunakan untuk menganalisa dengan cara mendeskripsikan atau memberi gambaran terhadap objek yang diteliti, kemudian hasilnya akan dianalisis berdasarkan teori dan norma hukum yang relevan. Data yang terkumpul dalam penelitian ini akan diolah oleh penulis. Data yang telah diolah akan ditinjau kembali dan dikelompok-kelompokkan melalui indikator-indikator tertentu.

F. Sistematika Penulisan

Sistematika Penulisan ini disajikan untuk mempermudah pembaca dalam memahami materi yang dibahas di tiap bab dari skripsi ini. Penulisan skripsi ini dibagi kedalam 5 bab sebagaimana akan diuraikan dibawah ini:

Bab pertama berisi pendahuluan mengenai latar belakang permasalahan topik skripsi ini. Adapun pendahuluan ini berisi latar belakang mengenai topik dalam judul, lalu rumusan masalah yang akan dibahas dan dijawab dalam bab pembahasan skripsi ini. Dalam skripsi ini, topik yang akan dibahas adalah bagaimana penerapan *Convention on Cybercrime* kepada Warga Negara Indonesia pelaku kejahatan peretasan transnasional.

---

[12] Sirajuddin Saleh, 2017, Analisis Data Kualitatif, Bandung: Pustaka Ramadhan, Hlm. 3, diakses pada tanggal 8 Juli 2022 dari http://eprints.unm.ac.id/14856/.

Bab kedua berisi tinjauan pustaka yang berfungsi sebagai penjelasan umum objek penelitian. Pada bab ini akan dijelaskan terlebih dahulu mengenai *Convention on Cybercrime*, kemudian dijelaskan pula kejahatan peretasan, lalu pengertian Warga Negara Indonesia pelaku peretasan.

Bab ketiga berisi tentang hasil penelitian dan pembahasan masalah yang dipilih. Penelitian dan pembahasan ini akan menjawab pertanyaan yang menjadi rumusan masalah pada bab pendahuluan.

Bab keempat berisi kesimpulan dari pembahasan dan saran penulis.

BAB II

TELAAH PUSTAKA

A. Convention on Cybercrime