

# KENDALA DALAM PENANGGULANGAN *CYBERCRIME* SEBAGAI SUATU TINDAK PIDANA KHUSUS

Oleh

I Made Agus Windara

AA. Ketut Sukranatha

Bagian Hukum Pidana Fakultas Hukum Universitas Udayana

## ABSTRAK

Seperti yang kita ketahui belakangan ini marak terjadi beragam kejahatan baik berdimensi nasional maupun internasional yang perlu mendapatkan perhatian khusus dari aparat penegak hukum. Salah satu kejahatan yang marak diperbincangkan yaitu kejahatan *Cybercrime* yang dapat dilakukan tanpa mengenal batas jarak ruang dan waktu sehingga dikenal juga dengan istilah *Kejahatan Mayantara*. *Cybercrime* ini merupakan sisi negatif dari dampak perkembangan teknologi yang kian canggih sehingga penanggulangan dari kejahatan tersebut memerlukan suatu keahlian dan pengetahuan khusus dalam bidang teknologi informasi.

**Kata Kunci: Teknologi Informasi, Kejahatan Dunia Maya, Tindak Pidana Khusus.**

## ABSTRACT

*As we know these days is rive variety of crimes in both national and international dimensions that need special attention from law enforcement. One discussed the rampant crime is cybercrime which can be done without knowing the limits of space and times so that the distance also known as mayantara Crime. Cybercrime is one of the negative side effects of the development of increasingly sophisticated technology that prevention of these crimes requires an expertise and specialized knowledge in the field of information technology.*

**Keywords: Information Technology, Cybercrime, Specific Crime.**

## I. PENDAHULUAN

### 1.1. Latar Belakang

*Cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Dengan adanya kemajuan teknologi tersebut sebagian orang dengan sangat mudah memasuki ruang lingkup kejahatan hanya dengan mengandalkan kemampuannya untuk menggerakkan sistem teknologi.

Terkait dengan hal tersebut Apabila kita berbicara mengenai peraturan perundang-undangan yang mengatur tentang *cybercrime* di Indonesia, bisa dibilang kita masih sangat tertinggal karena baru satu peraturan yang mengatur secara spesifik tentang *cybercrime*, yaitu Undang-Undang No.11 Tahun 2008 tentang Informasi dan Tentang Transaksi Elektronik (yang biasa disebut dengan UU ITE). Namun dengan adanya undang-undang itu belum dapat

menekan keberadaan *Cybercrime* karena masih terdapat kekurangan dalam Undang-Undang tersebut. Mengingat *Cybercrime* merupakan suatu kejahatan Mayantara yang dapat dilakukan tanpa mengenal batas ruang dan waktu, diperlukan suatu upaya pencegahan untuk menanggulangi kejahatan tersebut. Aktivitas pokok dari *cybercrime* adalah penyerangan terhadap *computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.

## **1.2. Tujuan**

Tujuan dari penulisan ini, disamping untuk mengetahui kebijakan dalam menanggulangi *cybercrime*, juga untuk mengetahui bagaimana efektivitas Undang-Undang No. 11 Tahun 2008 dalam menindak *cybercrime*.

## **II. ISI MAKALAH**

### **2.1 METODE PENELITIAN**

Jenis penelitian yang digunakan dalam penulisan yaitu penelitian hukum normatif. Penelitian ini mengkaji mengenai asas-asas hukum, sistematika hukum serta taraf sinkronisasi hukum.<sup>1</sup> Sumber bahan hukum yang digunakan dalam penelitian yaitu bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer yang digunakan dalam penulisan ini yaitu peraturan perundang-undangan sedangkan bahan hukum sekunder yang digunakan yaitu buku-buku ilmu hukum.<sup>2</sup> Jenis pendekatan yang digunakan dalam penelitian ini yaitu pendekatan perundang-undangan (*The Statute Approach*), pendekatan kasus (*The Case Approach*) dan pendekatan analisis konsep hukum (*Analytical and Conceptual Approach*). Analisis terhadap bahan hukum yang diperoleh penulis dilakukan dengan cara argumentative yang berdasarkan pada alasan-alasan yang bersifat penalaran hukum.

---

<sup>1</sup> Bambang Sunggono, 2010, *Metodologi Penelitian Hukum*, Rajawali Pers, Jakarta, hal.39.

<sup>2</sup> Bahder Johan Nasution, 2008, *Metode Penelitian Ilmu Hukum*, Mandar Maju, Bandung, hal.84.

## 2.2 HASIL DAN PEMBAHASAN

### 2.2.1. Beberapa Kebijakan Dalam Penanggulangan *Cybercrime* Dan Kendala Yang Dihadapi

Barda Nawawi Arief mengemukakan *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian masyarakat luas di dunia internasional. *Cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh kehidupan modern saat ini.<sup>3</sup>

Dalam Resolusi Kongres PBB VIII/1990 ditegaskan bahwa *Cybercrime* meliputi kejahatan sebagai berikut:

- a. Kejahatan dengan menggunakan sarana/sistem jaringan komputer.
- b. Kejahatan didalam sistem/jaringan komputer
- c. Kejahatan terhadap sistem/jaringan komputer.

Dalam rangka menanggulangi *Cybercrime*, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* mengajukan beberapa kebijakan antara lain sebagai berikut:

- a. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan
- b. Menghimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *Cybercrime*.
- c. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (Committee on Crime Prevention and Control) PBB.<sup>4</sup>

---

<sup>3</sup> Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, Raja Grafindo Persada, Jakarta, hal.26.

<sup>4</sup> Barda Nawawi Arief, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Kencana, Jakarta, hal. 247.

Walaupun Resolusi Kongres PBB VIII/1990 telah menghimbau negara anggota untuk menanggulangi *Cybercrime* dengan sarana penal, namun kenyataannya tidaklah mudah. Hal ini disebabkan oleh beberapa hal, yaitu:

- a. Perbuatan jahat yang dilakukan berada dilingkungan elektronik. Oleh karena itu penanggulangan *Cybercrime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara yang bersangkutan.
- b. *Cybercrime* melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah territorial negaranya sendiri.
- c. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *cybercrime*<sup>5</sup>. Terjadinya *data havens* (negara tempat berlindung/singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

### **2.2.2 Pemanfaatan Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik Dalam Menindak *Cybercrime***

Di Indonesia sendiri, telah ada ketentuan Undang-Undang yang mengatur masalah *cybercrime* yaitu Undang-Undang Nomor 11 Tahun 2009 Tentang Informasi dan Transaksi Elektronik. Dalam Undang-Undang ini terdapat beberapa persoalan yang menonjol yaitu:

1. Perihal pembuktian yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.
2. Berkaitan dengan penafsiran tentang asas-asas dan norma hukum ketika menghadapi persoalan kebendaan yang tidak berwujud.

Dalam kenyataannya *Cybercrime* bukan merupakan sesuatu yang sederhana, karena kegiatannya tidak lagi dibatasi oleh teritorial suatu negara. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi seperti pencurian dana kartu kredit melalui pembelian di internet (*carding*). Dalam *Cybercrime*

---

<sup>5</sup> *Ibid.*

pembuktian<sup>6</sup> merupakan faktor yang sangat penting mengingat informasi elektronik belum terakomodasi dalam sistem hukum acara pidana Indonesia.

Undang-undang ini, yang telah disahkan dan diundangkan pada tanggal 21 April 2008, walaupun sampai dengan hari ini belum ada sebuah Peraturan Pemerintah yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang-undang *cyber* atau *cyberlaw* guna menjerat pelaku-pelaku *cybercrime* yang tidak bertanggungjawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi dalam mencapai kepastian hukum.

### **III. KESIMPULAN**

Mengenai upaya penanggulangan *Cybercrime* memerlukan suatu perhatian dan keahlian khusus dalam bidang teknologi, karena kejahatan ini mempergunakan sistem jaringan komputer yang dapat digunakan oleh siapapun juga tanpa mengenal batas teritorial dan waktu. Terkait dengan hal tersebut di Indonesia telah memiliki Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam menindak kejahatan *Cybercrime*. Namun dalam pembuktian mengenai *cybercrime* Kitab Undang-Undang Hukum Acara Pidana belum mengatur mengenai informasi elektronik sebagai salah satu alat bukti. Sehingga diharapkan ketentuan mengenai informasi elektronik diatur secara tegas sehingga terdapat suatu kepastian hukum.

### **DAFTAR PUSTAKA**

Hamzah, Andi, 1983, *Pengantar Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta.

Nasution, Bahder Johan, 2008, *Metode Penelitian Ilmu Hukum*, Mandar Maju, Bandung.

Nawawi Arief, Barda, 2006, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, Raja Grafindo Persada, Jakarta.

-----, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*, Kencana, Jakarta.

Sunggono, Bambang, 2010, *Metodologi Penelitian Hukum*, Rajawali Pers, Jakarta.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

---

<sup>6</sup>Andi Hamzah, 1983, *Pengantar Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, hal.66.