

## PERANAN PENYIDIK DALAM TINDAK PIDANA CYBERCRIME<sup>1</sup>

Oleh: Hedriyanto Kusno Jacob<sup>2</sup>

### ABSTRAK

Tujuan dilakukannya penelitian ini adalah untuk mengetahui perbuatan-perbuatan apakah yang merupakan *cybercrime* yang dapat dipidana di Indonesia dan bagaimana peranan Penyidik dalam penyidikan tindak pidana *cybercrime*. Dengan menggunakan metode penelitian yuridis normatif, disimpulkan: 1. Perbuatan-perbuatan *cybercrime* yang dapat dipidana berdasarkan Pasal 27 sampai dengan Pasal 37 Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 telah mencakup hampir semua perbuatan yang dipandang sebagai *cybercrime* oleh para pengguna komputer dan internet, kecuali: 1) perbuatan yang merupakan *spam*; dan 2) perbuatan yang merupakan *cyberterrorism*. 2. Peranan Penyidik dalam penyidikan tindak pidana *cybercrime* yaitu: 1) mempunyai pengetahuan dasar mengenai sarana-sarana Teknologi Informasi dan Komunikasi; dan 2) mengoptimalkan penggunaan ahli untuk memberikan keterangan ahli dalam bidang Teknologi Informasi dan Komunikasi.

Kata kunci: Peranan Penyidik, Tindak Pidana, Cybercrime

### PENDAHULUAN

#### A. Latar Belakang

Indonesia telah membentuk antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian telah mendapat beberapa perubahan melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 19 Tahun 2016 ini tidak mencabut dan menggantikan Undang-Undang Nomor 11 Tahun 2006 melainkan hanya melakukan perubahan terhadap pasal-pasal tertentu dalam Undang-Undang Nomor 11 Tahun 2006.

Rumusan tindak pidana dalam Undang-Undang Nomor 11 Tahun 2006 diatur dalam Bab VII: Perbuatan Yang Dilarang, yang mencakup Pasal 27 sampai Pasal 37, sedangkan ancaman pidananya ditentukan dalam Bab XI: Ketentuan Pidana, yang mencakup Pasal 45 sampai dengan Pasal 52. Perubahan yang dilakukan oleh Undang-Undang Nomor 19 Tahun 2016 terhadap rumusan tindak pidana hanyalah mengenai untuk penjelasan Pasal 27 dan rumusan Pasal 31 ayat (3) dan ayat (4).

Uraian sebelumnya menimbulkan pertanyaan apakah perbuatan-perbuatan yang pada umumnya dipandang sebagai *cybercrime* dan apakah perbuatan-perbuatan tersebut telah dapat dicakup oleh Pasal 27 sampai dengan Pasal 37 Undang-Undang Nomor 11 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Selain itu perbuatan-perbuatan yang merupakan *cybercrime*, sebagaimana dikemukakan sebelumnya, amat beranekaragam dan cukup rumit berkenaan dengan pembuktian menurut hukum acara pidana, sehingga memerlukan keterampilan dari Penyidik berkenaan dengan masalah-masalah komputer dan internet. Dengan latar belakang tersebut maka dalam rangka penulisan skripsi, pokok tersebut telah dipilih untuk dibahas di bawah judul "Peran Penyidik dalam Tindak Pidana Cybercrime".

#### B. Rumusan Masalah

1. Perbuatan-perbuatan apakah yang merupakan *cybercrime* yang dapat dipidana di Indonesia?
2. Bagaimana peranan Penyidik dalam penyidikan tindak pidana *cybercrime*?

#### C. Metode Penelitian

Penelitian ini merupakan suatu penelitian hukum normatif, yaitu penelitian dengan terutama melihat hukum sebagai seperangkat norma (*a set of rules*), di mana penelitian ini dikenal juga dengan nama penelitian kepustakaan (*library research*).

### PEMBAHASAN

#### A. Cybercrime Yang Dapat Dipidana di Indonesia

Rumusan dari perbuatan-perbuatan yang dapat dipidana diatur dalam Bab VII: Perbuatan

<sup>1</sup> Artikel Skripsi. Dosen Pembimbing : Dr. Merry E. Kalalo, SH, M; Dr. Ruddy R. Watulingas, SH, MH

<sup>2</sup> Mahasiswa pada Fakultas Hukum Unsrat, NIM. 100711451

Yang Dilarang dari Undang-Undang Nomor 11 Tahun 2008, yang mencakup Pasal 27 sampai dengan Pasal 37, sedangkan ancaman pidana terhadap perbuatan-perbuatan yang bersangkutan diatur dalam Bab XI: Ketentuan Pidana, yang meliputi Pasal 45 sampai dengan Pasal 52. Terhadap pasal-pasal ini, oleh Undang-Undang Nomor 19 Tahun 2016 ada dilakukan sedikit perubahan, yaitu: (1) Perubahan terhadap penjelasan dari Pasal 27 ayat (1), ayat (3), dan ayat (4); dan (2) Perubahan terhadap Pasal 31 ayat (3) dan ayat (4).

Perbuatan-perbuatan yang merupakan tindak pidana menurut Pasal 27 sampai dengan Pasal 37 serta perubahannya dapat diuraikan satu persatu sebagai berikut.

**1. Pasal 27 Undang-Undang Nomor 11 Tahun 2008 serta perubahan atas penjelasan Pasal 27 ayat (1), ayat (3) dan ayat (4) menurut Undang-Undang Nomor 19 Tahun 2016.**

Perubahan yang dilakukan oleh Undang-Undang Nomor 19 Tahun 2016 bukanlah terhadap rumusan Pasal 27, melainkan perubahan terhadap penjelasan Pasal 27 khususnya terhadap penjelasan Pasal 27 ayat (1), ayat (3), dan ayat (4). Dengan demikian, rumusan Pasal 27 itu sendiri tidak mengalami perubahan.

Pasal 27 Undang-Undang Nomor 11 Tahun 2008 memberikan ketentuan,

- (1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesucilaan.
- (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
- (3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

- (4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.<sup>3</sup>

**2. Pasal 28 Undang-Undang Nomor 11 Tahun 2008**

Pasal 28 Undang-Undang Nomor 11 Tahun 2008 memberikan ketentuan sebagai berikut,

- (1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
- (2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 28 ayat (1) dan ayat (2) ini merupakan penyebaran berita tidak benar, yang mengakibatkan kerugian terhadap konsumen (Pasal 28 ayat 1) atau ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, rasm dan antargolongan (SARA). Penyebaran berita bohong ini dalam *cybercrime* disebut sebagai *hoax*, sehingga dapat dikatakan Undang-Undang Nomor 11 Tahun 2008 dalam Pasal 28 telah mencakup perbuatan yang dalam *cybercrime* disebut *hoax* sebagaimana telah dikemukakan dalam Bab II huruf B.

**3. Pasal 29 Undang-Undang Nomor 11 Tahun 2008.**

Pasal 29 Undang-Undang Nomor 11 Tahun 2008 menentukan bahwa, Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen

<sup>3</sup> Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran negara Republik Indonesia Nomor 4843).

Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Unsur-unsur pasal ini terdiri atas:

- a. Setiap Orang;
- b. dengan sengaja;
- c. dan tanpa hak;
- d. mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik;
- e. yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Jadi ancaman kekerasan atau menakut-nakuti ini bukan ditujukan kepada banyak orang, melainkan ditujukan **secara pribadi**, atau kepada orang tertentu saja.

Rumusan Pasal 29 Undang-Undang Nomor 11 Tahun 2008 ini memiliki unsur perbuatan perbuatan “mengirim Informasi Elektronik dan/atau Dokumen Elektronik” sedangkan informasi/Dokumen Elektronik itu berisi “ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi”. Isi Informasi/Dokumen Elektronik menunjukkan bahwa pelaku melakukan cyberstalking atau cyberbullying terhadap seorang tertentu. Dengan demikian, pasal ini telah dapat mencakup perbuatan yang dalam *cybercrime* disebut sebagai *cyberstalking* atau *cyberbullying* sebagaimana telah dikemukakan dalam Bab II huruf B skripsi.

#### 4. Pasal 30 Undang-Undang Nomor 11 Tahun 2008.

Pasal 30 Undang-Undang Nomor 11 Tahun 2008 memberikan ketentuan sebagai berikut,

- (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.<sup>4</sup>

Rumusan pasal ini menunjukkan pelaku mengakses komputer milik orang lain. Perbuatan ini merupakan **penerobosan jaringan komputer (*hacking, peretasan*)** sebagaimana telah diuraikan dalam Bab II huruf B skripsi ini. Dengan demikian, Pasal 30 ini telah mencakup *cybercrime* berupa penerobosan jaringan komputer (*hacking, peretasan*).

#### 5. Pasal 31 Undang-Undang Nomor 11 Tahun 2008.

Dalam Pasal 31 Undang-Undang Nomor 11 Tahun 2008 ditentukan bahwa,

- (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 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) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

<sup>4</sup> Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran negara Republik Indonesia Nomor 4843).

- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

#### **6. Pasal 32 Undang-Undang Nomor 11 Tahun 2008**

Pasal 32 Undang-Undang Nomor 11 Tahun 2008 memberikan ketentuan bahwa,

- (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.

Perbuatan yang dilarang dalam Pasal 32 Undang-Undang Nomor 11 Tahun 2008 ini merupakan salah satu bentuk penerobosan jaringan komputer (*hacking*, peretasan), di mana yang bersifat khusus dalam hal ini yaitu pelaku sesudah melakukan *hacking* (peretasan) kemudian menyembunyikan Informasi/Dokumen Elektronik atau mengirimkannya kepada pihak lain yang tidak berhak. Dengan demikian, Pasal ini juga menunjukkan telah dicakupnya perbuatan penerobosan jaringan komputer (*hacking*, peretasan) dalam *cybercrime* sebagaimana telah diuraikan dalam Bab II huruf B skripsi ini.

#### **7. Pasal 33 Undang-Undang Nomor 11 Tahun 2008**

Dalam Pasal 33 Undang-Undang Nomor 11 Tahun 2008 ditentukan bahwa, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Perbuatan yang dilarang dalam Pasal 33 Undang-Undang Nomor 11 Tahun 2008 ini merupakan pembuatan dan penyebaran dari virus dan program-program sejenis yang jahat lainnya (*worm*, *trojan horse*, *backdoor*, *spyware*, *joke*) yang sangat dikenal dalam *cybercrime*. Dengan demikian, Pasal 33 ini telah mencakup pembuatan dan penyebaran dari virus dan program-program sejenis yang jahat lainnya (*worm*, *trojan horse*, *backdoor*, *spyware*, *joke*) sebagaimana telah diuraikan dalam Bab II huruf B skripsi ini.

#### **8. Pasal 34 Undang-Undang Nomor 11 Tahun 2008**

Pasal 34 Undang-Undang Nomor 11 Tahun 2008 menentukan sebagai berikut,

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
  - a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
  - b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
- (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik

itu sendiri secara sah dan tidak melawan hukum.

Perbuatan yang dirumuskan dalam Pasal 34 ayat (1) merupakan perbuatan komersial untuk menyediakan perangkat keras (hardware), yaitu “semua bagian fisik komputer”,<sup>5</sup> dan perangkat lunak (software), yaitu “program komputer”,<sup>6</sup> yang dapat digunakan untuk memfasilitasi perbuatan yang diuraikan dalam Pasal 27 sampai dengan Pasal 33 Undang-Undang Nomor 11 Tahun 2008.

#### **9. Pasal 35 Undang-Undang Nomor 11 Tahun 2008**

Dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 ditentukan bahwa, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Perbuatan yang dirumuskan dalam Pasal 35 ini merupakan salah satu bentuk penipuan, yaitu melakukan perubahan terhadap Informasi/Dokumen Elektronik milik orang lain tetapi dengan maksud agar orang-orang lainnya mengira itu merupakan Informasi/Dokumen Elektronik yang asli. Perbuatan ini dapat dikatakan telah mencakup perbuatan penipuan melalui dunia maya (*cyberspace*) yang telah diuraikan dalam Bab II huruf B skripsi ini.

#### **10. Pasal 36 Undang-Undang Nomor 11 Tahun 2008**

Dalam Pasal 36 Undang-Undang Nomor 11 Tahun 2008 diberikan ketentuan bahwa, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27

sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Rumusan pasal ini menunjukkan bahwa perbuatan yang dimaksudkan di sini yaitu bersifat pemberatan terhadap perbuatan-perbuatan yang telah dirumuskan dalam Pasal 27 sampai dengan Pasal 34. Perbuatan yang dirumuskan dalam Pasal 27 sampai dengan Pasal 34 ada kemungkinan tidak sempat menimbulkan kerugian bagi orang lain, tetapi Pasal 36 mengatur kemungkinan pemberatan jika perbuatan-perbuatan tersebut menimbulkan kerugian bagi orang lain.

#### **11. Pasal 37 Undang-Undang Nomor 11 Tahun 2008**

Paal 37 Undang-Undang Nomor 11 Tahun 2008 memberikan ketentuan bahwa, Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

#### **B. Peranan Penyidik dalam Penyidikan Tindak Pidana Cybercrime**

Peran utama Penyidik adalah melakukan penyidikan, yaitu “serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya”<sup>7</sup> (Pasal 1 angka 2 KUHAP). Jadi, peran utama Penyidik yaitu mencari serta mengumpulkan bukti yang dengan bukti itu: 1) membuat terang tentang tindak pidana yang terjadi, dan 2) guna menemukan tersangkanya.

Bukti yang dicari dan dikumpulkan oleh Penyidik itu mencakup alat bukti dan barang bukti. Alat bukti merupakan alat yang ditentukan oleh undang-undang sebagai dasar untuk pembuktian perkara pidana. Sebagaimana dikatakan oleh Andi Hamzah,

<sup>5</sup> Wikipedia Bahasa Indonesia. “Perangkat Keras”. [https://id.wikipedia.org/wiki/Perangkat\\_keras](https://id.wikipedia.org/wiki/Perangkat_keras). Diakses tanggal 15/05/2017.

<sup>6</sup> M. Arsyad Sanusi. 2005. *Hukum dan Teknologi Informasi*. Jakarta: Tim KemasBuku. Hlm. 74.

<sup>7</sup> Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3209).

Menurut Pasal 184 KUHAP, alat-alat bukti ialah:

- a. keterangan saksi;
- b. keterangan ahli;
- c. surat;
- d. petunjuk;
- e. keterangan terdakwa.<sup>8</sup>

Masing-masing alat bukti tersebut menjadi dasar untuk pembuktian suatu perkara pidana. Dalam KUHAP juga ada ketentuan bahwa Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya (Pasal 183 KUHAP).

Barang bukti (Lat.: *corpus delicti*) adalah "objek suatu tindak pidana, benda pada atau dengan mana suatu tindak pidana dilakukan".<sup>9</sup> Barang bukti ini mencakup: 1) objek suatu tindak pidana, misalnya suatu barang yang dirusakkan oleh pelaku dalam tindak pidana perusakan barang, 2) benda dengan mana suatu tindak pidana dilakukan, misalnya suatu pisau yang digunakan untuk melakukan penganiayaan, dan 3) benda hasil suatu tindak pidana, misalnya uang hasil perampokan.

Dalam *cybercrime* semua alat bukti dan barang bukti menjadi hal penting untuk pembuktian, tetapi ada hal yang bersifat khusus untuk *cybercrime* karena dalam *cybercrime* pada umumnya dilibatkan Teknologi Informasi dan Komunikasi. Mengenai Teknologi Informasi dan Komunikasi ini dalam suatu artikel dikemukakan bahwa,

**Teknologi Informasi dan Komunikasi**, adalah payung besar terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi. TIK mencakup dua aspek yaitu teknologi informasi dan teknologi komunikasi. Teknologi informasi meliputi segala hal yang berkaitan dengan proses, penggunaan sebagai alat bantu, manipulasi, dan pengelolaan informasi. Sedangkan teknologi komunikasi adalah segala sesuatu

yang berkaitan dengan penggunaan alat bantu untuk memproses dan mentransfer data dari perangkat yang satu ke lainnya. Oleh karena itu, teknologi informasi dan teknologi komunikasi adalah dua buah konsep yang tidak terpisahkan. Jadi Teknologi Informasi dan Komunikasi mengandung pengertian luas yaitu segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, pemindahan informasi antar media. Istilah TIK muncul setelah adanya perpaduan antara teknologi komputer (baik perangkat keras maupun perangkat lunak) dengan teknologi komunikasi pada pertengahan abad ke-20. Perpaduan kedua teknologi tersebut berkembang pesat melampaui bidang teknologi lainnya. Hingga awal abad ke-21, TIK masih terus mengalami berbagai perubahan dan belum terlihat titik jenuhnya.<sup>10</sup>

Pembuktian tindak pidana *cybercrime* yang melibatkan Teknologi Informasi dan Komunikasi, dengan sendirinya membutuhkan pengetahuan dan keahlian dalam bidang Teknologi Informasi dan Komunikasi. Penyidik pada umumnya merupakan Polisi yang dilatih dalam bidang hukum, bukan dalam bidang Teknologi Informasi dan Komunikasi. Oleh karenanya, peranan Penyidik dalam penyidikan tindak pidana *cybercrime* yaitu: 1) mempunyai pengetahuan dasar mengenai sarana-sarana Teknologi Informasi dan Komunikasi; dan 2) mengoptimalkan penggunaan ahli untuk memberikan keterangan ahli dalam bidang Teknologi Informasi dan Komunikasi. Dengan 2 (dua) peranan ini maka lebih besar kemungkinan untuk mencari dan mengumpulkan bukti, baik alat bukti maupun barang bukti berupa dokumen elektronik, yang dengan bukti itu membuat terang tentang tindak pidana *cybercrime* yang terjadi, dan menemukan tersangkanya.

## PENUTUP

### A. Kesimpulan

<sup>8</sup> Andi Hamzah. 2014. *Hukum Acara Pidana di Indonesia*. Ed.2 cet.8. Jakarta: Sinar Grafika. Hlm. 259.

<sup>9</sup> R. Subekti dan Tjitrosudibio. *Op.cit.* Hlm. 30.

<sup>10</sup> Wikipedia Bahasa Indonesia. "Teknologi Informasi dan Komunikasi". [https://id.wikipedia.org/wiki/Teknologi\\_Informasi\\_Komunikasi](https://id.wikipedia.org/wiki/Teknologi_Informasi_Komunikasi). Diakses tanggal 15/05/2017.

1. Perbuatan-perbuatan *cybercrime* yang dapat dipidana berdasarkan Pasal 27 sampai dengan Pasal 37 Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 telah mencakup hampir semua perbuatan yang dipandang sebagai *cybercrime* oleh para pengguna komputer dan internet, kecuali: 1) perbuatan yang merupakan *spam*; dan 2) perbuatan yang merupakan *cyberterrorism*.
2. Peranan Penyidik dalam penyidikan tindak pidana *cybercrime* yaitu: 1) mempunyai pengetahuan dasar mengenai sarana-sarana Teknologi Informasi dan Komunikasi; dan 2) mengoptimalkan penggunaan ahli untuk memberikan keterangan ahli dalam bidang Teknologi Informasi dan Komunikasi.

#### B. Saran

1. Perlu dibuat ketentuan yang mengancamkan pidana terhadap perbuatan yang merupakan *cyberterrorism*.
2. Penting meningkatkan kemampuan Penyidik Polri sampai yang bertugas di kota-kota kecil untuk mempunyai pengetahuan dasar tentang sarana-sarana Teknologi Informasi dan Komunikasi, dan perlunya perguruan tinggi mempunyai tenaga-tenaga ahli untuk memberikan keterangan ahli dalam bidang Teknologi Informasi dan Komunikasi.

#### DAFTAR PUSTAKA

- Andi Hamzah. 2014. *Hukum Acara Pidana di Indonesia*. Ed.2 cet.8. Jakarta: Sinar Grafika.
- Bambang Poernomo. 1978. *Asas-asas Hukum Pidana*. Jakarta: Ghalia Indonesia.
- Djoko Prakoso. 1987. *Penyidik, Penuntut Umum, Hakim, dalam Proses Hukum Acara Pidana*. Jakarta: Bina Aksara.
- Lamintang, P.A.F. dan C.D. Samosir. 1983. *Hukum Pidana Indonesia*. Bandung: Sinar Baru.
- Lamintang, P.A.F. dan F.T. Lamintang. 2014. *Dasar-dasar Hukum Pidana di Indonesia*. Jakarta: Sinar Grafika.
- M. Arsyad Sanusi. 2005. *Hukum dan Teknologi Informasi*. Jakarta: Tim KemasBuku.
- Mahrus Ali. 2012. *Dasar-dasar Hukum Pidana*. Cet.2. Jakarta: Sinar Grafika.
- Maramis, Frans. 2012. *Hukum Pidana Umum dan Tertulis di Indonesia*. Jakarta: Rajawali Pers.
- R. Subekti dan Tjitrosudibio. 2003. *Kamus Hukum*. Cet.15. Jakarta: Pradnya Paramita.
- R. Tresna. 1959. *Azas-azas Hukum Pidana*. Jakarta: Tiara Ltd.
- \_\_\_\_\_. 1976. *Komentar H.I.R.* Cet.6, Jakarta: Pradnya Paramita.
- Sianturi, S.R. 1983. *Tindak Pidana di KUHP Berikut Uraianya*. Jakarta: Alumni AHM-PTHM.
- Soerjono Soekanto dan Sri Mamudji. 2014. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Cet.16. Jakarta: Rajawali Pers.
- Teguh Prasetyo. 2013. *Hukum Pidana*. Cet.4. Jakarta: Rajawali Pers.
- Tim Penerjemah BPHN. 1983. *Kitab Undang-Undang Hukum Pidana*. Jakarta: Sinar Harapan.
- Tim Penyusun Kamus Pusat Bahasa. 2002. *Kamus Besar Bahasa Indonesia*. Ed. 3 cet. 2. Jakarta: Balai Pustaka.
- Utrecht, E. 1967. *Hukum Pidana I*. Bandung: Penerbitan Universitas.
- Wirjono Prodjodikoro. 1981. *Asas-asas Hukum Pidana di Indonesia*. Cet.3. Jakarta-Bandung: Eresco.
- \_\_\_\_\_. 1981. *Hukum Acara Pidana di Indonesia*. Cet. 10. Bandung: Sumur Bandung.
- \_\_\_\_\_. 2012. *Tindak-tindak Pidana Tertentu di Indonesia*. Ed.3 Cet.4. Bandung: Refika Aditama.

#### Sumber Internet/Dokumen Elektronik:

- Brenner, Susan W. 1981. "Is There Such a Thing as 'Virtual Crime'?". J.D. – Indiana University.  
<http://boalt.org/CCLR/v4/v4brenner.htm>. Diakses tanggal 11/05/2017.
- Overholt, Matt. "Overview of Cyber-Terrorism".  
<http://cybercrimes.net/Terrorism/overview/page1.html>. Diakses tanggal 11/05/2017.

Wikipedia. "Stalking".  
<https://en.wikipedia.org/wiki/Stalking>.  
Diakses tanggal 12/05/2017.

Wikipedia. "Cyberstalking".  
<https://en.wikipedia.org/wiki/Cyberstalking>.  
Diakses tanggal 12/05/2017.

Wikipedia Bahasa Indonesia. "Kejahatan Dunia Maya".  
[https://id.wikipedia.org/wiki/Kejahatan\\_dunia\\_maya](https://id.wikipedia.org/wiki/Kejahatan_dunia_maya). Diakses tanggal 09/05/2017.

Wikipedia Bahasa Indonesia. "Pemberitaan Palsu".  
[https://id.wikipedia.org/wiki/Pemberitaan\\_palsu](https://id.wikipedia.org/wiki/Pemberitaan_palsu). Diakses tanggal 12/05/2017.

Wikipedia Bahasa Indonesia. "Pembuntutan Dunia Maya".  
[https://id.wikipedia.org/wiki/Pembuntutan\\_dunia\\_maya](https://id.wikipedia.org/wiki/Pembuntutan_dunia_maya). Diakses tanggal 12/05/2017.

Wikipedia Bahasa Indonesia. "Perangkat Keras".  
[https://id.wikipedia.org/wiki/Perangkat\\_keras](https://id.wikipedia.org/wiki/Perangkat_keras). Diakses tanggal 15/05/2017.

Wikipedia Bahasa Indonesia. "Peretas".  
<https://id.wikipedia.org/wiki/Peretas>.  
Diakses tanggal 12/05/2017.

Wikipedia Bahasa Indonesia. "Teknologi Informasi dan Komunikasi".  
[https://id.wikipedia.org/wiki/Teknologi\\_Informasi\\_Komunikasi](https://id.wikipedia.org/wiki/Teknologi_Informasi_Komunikasi). Diakses tanggal 15/05/2017.

Wikipedia Bahasa Indonesia. "Virus Komputer".  
[https://id.wikipedia.org/wiki/Virus\\_komputer](https://id.wikipedia.org/wiki/Virus_komputer).  
Diakses tanggal 12/05/2017.

**Peraturan Perundang-undangan:**

Undang-Undang Nomor 13 Tahun 1961 tentang Ketentuan-ketentuan Pokok Kepolisian Negara (Lembaran Negara Republik Indonesia Tahun 1961 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 2289).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3209).

Undang-Undang Nomor 5 Tahun 1983 tentang Zona Ekonomi Eksklusif Indonesia (Lembaran Negara Republik Indonesia Tahun 1983 Nomor 44, Tambahan

Lembaran Negara Republik Indonesia Nomor 3260).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran negara Republik Indonesia Nomor 4843).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Peraturan Pemerintah Nomor 27 Tahun 1983 tentang Pelaksanaan Kitab Undang-Undang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1983 Nomor 36, Tambahan Lembaran Negara Republik Indonesia Nomor 3258).