



ANALISIS YURIDIS TINDAKAN MENGAKSES INFORMASI ELEKTRONIK SECARA ILEGAL BERDASARKAN KEBIJAKAN HUKUM PIDANA DI INDONESIA

Achmad Nosi Utama*, Nyoman Serikat Putra Jaya, Purwoto
Program Studi S1 Ilmu Hukum, Fakultas Hukum, Universitas Diponegoro
E-mail : nosiutama@gmail.com

Abstrak

Salah satu konsekuensi dari perkembangan teknologi informasi yaitu semakin mudahnya suatu pihak untuk mengakses Informasi Elektronik secara ilegal. Sebagai Negara Hukum, Indonesia memiliki kewajiban untuk memberikan aturan hukum untuk menanggulangi tindakan mengakses Informasi Elektronik secara ilegal tersebut. Sehingga, penulisan ini bertujuan untuk mengetahui kebijakan formulasi terhadap perbuatan mengakses Informasi Elektronik secara ilegal berdasarkan hukum positif Indonesia dan untuk mengkaji kebijakan formulasi dalam penanggulangan perbuatan mengakses Informasi Elektronik secara ilegal berdasarkan hukum di Indonesia yang lebih baik pada masa yang akan datang.

Berdasarkan hasil penelitian ini, diperoleh hasil bahwa tindakan mengakses Informasi Elektronik secara ilegal dirumuskan sebagai suatu tindak pidana, yang diatur dalam Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, dan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Kebijakan formulasi terhadap tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum di Indonesia yang akan datang sudah mulai diatur melalui Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012. Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012 tersebut memiliki aturan yang lebih lengkap dibandingkan Peraturan Perundang-undangan di Indonesia saat ini. Oleh karena itu, pemberlakuan Kitab Undang-undang Hukum Pidana Indonesia perlu dilakukan secepatnya.

Kata kunci : Akses Ilegal, Informasi Elektronik, Kebijakan Hukum Pidana

Abstract

One consequence of the development of information technology is the easy party to access the Electronic Information illegally. As the State of Law, Indonesia has an obligation to provide the rule of law to tackle illegal actions to access the information. Thus, this paper aims to determine the policy formulation of the act of illegally accessing Electronic Information based on the positive law in Indonesia and to assess the policy formulation in the prevention of acts illegally accessing Electronic Information based on the law in Indonesia better in the future.

Based on these results, the result that the action accessing electronic information illegally formulated as a criminal offense regulated in Law Number 36 Year 1999 on Telecommunication, Law Number 23 Year 2006 concerning Population Administration, Law No. 14 of 2008 on Public Information, and Law No. 11 Year 2008 on Information and Electronic Transactions.

Policy formulation to act illegally accessing electronic information under criminal law in Indonesia that will come already started to be regulated through the draft the Code of Criminal Indonesia Year 2012. The design of the Code of Criminal Indonesia 2012 have a rule that is more complete than Laws -undangan in Indonesia today. Therefore, the implementation of the Code of Criminal Indonesia needs to be done as soon as possible.

Keywords : Illegal access, electronic information, Criminal Law Policy



I. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi saat ini, membuat akses terhadap informasi sangat mudah untuk dilakukan, baik informasi dalam skala global, hingga informasi yang sangat privat. Perkembangan tersebut salah satunya dalam bentuk perkembangan di bidang teknologi informasi. Perkembangan teknologi informasi yang pesat, menyebabkan suatu dampak positif dan negatif. Sehingga, perkembangan teknologi informasi ini diibaratkan dengan pedang bermata dua. Dikatakan sebagai pedang bermata dua, karena selain memberi kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif bagi perbuatan melawan hukum.

Beberapa contoh perbuatan melawan hukum dengan menggunakan sarana teknologi informasi yaitu prostitusi online, perjudian online, dan pencemaran nama melalui internet. Perbuatan melawan hukum tersebut biasa disebut dengan *cybercrime* atau menurut Barda Nawawi Arief disebut dengan tindak pidana mayantara.¹

Sebagai negara hukum, Negara Indonesia memiliki kewajiban untuk mengatur tata kehidupan di negara ini dengan sebuah aturan yang disebut hukum, termasuk pengaturan tentang *cybercrime*. Hukum tersebut dapat menjadi sarana untuk melakukan pengaturan bagi setiap masyarakat agar lebih bijak dalam

mempergunakan teknologi, sehingga penggunaannya tidak melanggar Hak Asasi Manusia dan tidak bertentangan dengan Pancasila serta Undang-undang Dasar Negara Indonesia Tahun 1945.

Salah satu konsekuensi atas kemajuan teknologi informasi yaitu timbulnya beberapa informasi-informasi dalam bentuk elektronik yang disebut Informasi Elektronik. Pasal 1 angka 1 Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik memberi definisi mengenai Informasi Elektronik, yaitu:

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDJ), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Informasi Elektronik yang ada tersebut sangat rawan untuk diakses dengan mudah oleh pihak yang tidak memiliki hak untuk mengaksesnya. Artinya, berpotensi terjadi perbuatan akses Informasi Elektronik secara ilegal.

Pasal 1 ayat (3) Undang-undang Dasar Republik Indonesia Tahun 1945 menyebutkan bahwa Negara Indonesia adalah negara hukum. Sehingga menarik apabila peneliti melakukan penelitian terhadap kebijakan formulasi dalam hukum positif di Indonesia, tentang

¹ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta : PT Rajagrafindo Persada, 2013), Halaman 11.



bagaimana perlindungan Informasi Elektronik milik seseorang yang diakses oleh orang lain, tanpa izin atau secara ilegal. Sehingga nantinya dapat diketahui bagaimana atau sejauh mana Negara Indonesia melakukan perlindungan terhadap Informasi Elektronik melalui suatu kebijakan formulasi atau suatu regulasi, dan juga dapat diketahui apakah Negara Indonesia sudah sejalan dengan amanat Undang-undang Dasar Negara Republik Indonesia Tahun 1945, yang mengamanatkan bahwa Negara Indonesia adalah negara hukum.

Kemudian, dalam rangka evaluasi dan pengembangan kebijakan formulasi dalam hukum positif di Indonesia, akan dilakukan kajian perbandingan mengenai pengaturan tentang perbuatan mengakses Informasi Elektronik secara ilegal di Indonesia dengan negara lain.

Sehingga, dengan adanya kajian perbandingan tersebut, diharapkan dapat ditemukan kelemahan atau kekurangan dalam kebijakan formulasi hukum positif di Indonesia, yang kemudian dapat ditemukan juga solusi-solusi untuk melakukan pembaharuan ke arah yang lebih baik terhadap kebijakan formulasi dalam hukum positif di Indonesia dalam masa yang akan datang.

Berdasarkan uraian latar belakang di atas, maka permasalahan yang dapat disusun antara lain:

1. Bagaimanakah kebijakan formulasi terhadap tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum positif di Indonesia?

2. Bagaimanakah kebijakan formulasi dalam penanggulangan tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum di Indonesia pada masa yang akan datang?

II. METODE

Penelitian ini menggunakan pendekatan Yuridis Normatif, yaitu dengan mengkaji dengan memahami hukum sebagai perangkat peraturan atau norma-norma positif di dalam sistem perundang-undangan yang mengatur mengenai kehidupan manusia. Kemudian, penelitian ini didukung dengan pendekatan komparatif yaitu penelitian tentang perbandingan hukum baik mengenai perbandingan sistem hukum antar negara, maupun perbandingan produk hukum dan karakter hukum antar waktu dalam suatu negara.² Jadi penelitian ini dipahami sebagai penelitian kepustakaan, yaitu penelitian terhadap data sekunder.³

Spesifikasi penelitian ini adalah penelitian deskriptif analitis yang merupakan penelitian untuk menggambarkan dan menganalisa masalah yang ada dan termasuk dalam jenis penelitian kepustakaan (*library research*) yang akan disajikan secara deskriptif.

² Diakses dari situs: www.lawismayway.blogspot.com/2011/1/penelitian-atau-pengkajian-ilmu-hukum.html?m=1

³ Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, (Jakarta:Rajawali, 1985), Halaman 15.



III. HASIL DAN PEMBAHASAN

A. Kebijakan Terhadap Mengakses Elektronik Secara Ilegal Berdasarkan Hukum Pidana di Indonesia saat ini

1. Informasi Elektronik sebagai privasi yang harus dilindungi

Perkembangan ilmu pengetahuan dan teknologi yang terjadi saat ini, perlu diimbangi dengan pemenuhan sisi keamanan. Sehingga dalam pemanfaatan teknologi informasi, media, dan komunikasi, setiap orang tidak melakukan perbuatan yang bertentangan dengan Hak Asasi Manusia. Menurut Niniek Suparni, terdapat tiga pendekatan untuk menjaga keamanan di *cyberspace*, yaitu:⁴

- a. Pendekatan aspek hukum;
- b. Pendekatan aspek teknologi; dan
- c. Pendekatan aspek sosial budaya dan etika.

Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum persoalan teknologi informasi menjadi tidak optimal.⁵

Sebagai contoh penggunaan teknologi informasi dalam aktifitas masyarakat adalah penggunaan pesan elektronik (*email*) untuk berkirim

pesan, percakapan yang dilakukan dengan media handphone, dan penyimpanan dokumen-dokumen elektronik di dalam komputer. Pesan elektronik (*email*), percakapan, atau dokumen-dokumen di dalam komputer, merupakan beberapa bentuk dari Informasi Elektronik, dimana dengan perkembangan teknologi informasi yang pesat ini, hal tersebut rentan diakses oleh orang lain tanpa sizin pemiliknya.

Perbuatan mengakses Informasi Elektronik milik orang lain tanpa izin tersebut, merupakan perbuatan yang melanggar Hak Asasi Manusia. Dikatakan bahwa perbuatan tersebut merupakan perbuatan yang melanggar Hak Asasi Manusia, karena Informasi Elektronik merupakan salah satu bentuk privasi seseorang yang harus dilindungi oleh hukum.

Pasal 28 F Undang-undang Dasar Negara Republik Indonesia Tahun 1945 mengatur bahwa:

“Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia”.⁶

Pasal 28 F Undang-undang Dasar Negara Republik Indonesia Tahun 1945 tersebut mengatur bahwa kebebasan memperoleh informasi merupakan salah satu Hak Asasi Manusia yang harus dilindungi. Namun, kebebasan

⁴ Niniek Suparni, *Cyberspace Problematika Antisipasi Pengaturannya*, (Jakarta: Sinar Grafika, 2009), Halaman 111.

⁵ *Ibid.*

⁶ Lihat Pasal 28 F Undang-undang Dasar Negara Republik Indonesia Tahun 1945.



memperoleh informasi adalah hak asasi yang harus berakhir apabila muncul garis embarkasi perlindungan terhadap hak-hak pribadi.⁷

Kebebasan memperoleh informasi memiliki keterkaitan yang sangat erat dengan pemahaman hak-hak pribadi atau hak-hak privat atau hak-hak privasi (*privacy rights*). *Privacy* berkaitan dengan beragam bentuk dan privasi mengatur bagaimana seorang manusia memberikan akses kepada orang lain untuk mendapatkan informasi pribadinya, mengambil bagian dari kepemilikan pribadi dan keputusan pribadi. Hak-hak pribadi atau hak-hak privat (*privacy right*) dapat diartikan sebagai hak otonom yang dimiliki seseorang.⁸

Untuk mempermudah mempelajari privasi, beberapa pakar membagi privasi ke dalam 4 (empat) kategori, yaitu:⁹

1. *Information privacy*

Privasi yang mengatur tentang pengumpulan dan pengelolaan data atau data privasi seperti informasi tentang keuangan dan informasi tentang kesehatan seseorang.

2. *Bodily privacy*

Privasi atas tubuh seseorang seperti privasi atas DNA, Data Biometrik seseorang seperti retina mata dan sidik jari.

3. *Communication privacy*

Privasi atas komunikasi seseorang seperti surat, telepon, email atau bentuk komunikasi lainnya.

4. *Territorial privacy*

Privasi atas tempat tinggal seseorang, tempat bekerja.

Berdasarkan penjelasan di atas, dapat diketahui bahwa terdapat 2 (dua) kategori privasi yang berkaitan dengan perlindungan terhadap Informasi Elektronik, yaitu *Communication privacy* dan *Information Privacy*.

Selanjutnya, akan dijabarkan beberapa instrumen internasional yang melakukan perlindungan terhadap privasi, yaitu sebagai berikut:

1.1. **Deklarasi Universal tentang Hak Asasi Manusia Tahun 1948 (*Universal Declaration of Human Rights*)**

Perlindungan privasi di dalam Deklarasi Universal tentang Hak Asasi Manusia 1948 (*Universal Declaration of Human Rights*), terdapat di *Article 12*.

1.2. **Kovenan Internasional tentang Hak-hak Sipil dan Politik Tahun 1966 (*International Covenant on Civil and Political Rights*)**

Kovenan Internasional tentang Hak-hak Sipil dan Politik Tahun 1966 (*International Covenant on Civil and Political Rights*) memberikan perlindungan terhadap

⁷ Ninik Suparni, *Loc.cit.*

⁸ Danrivanto Budhijanto, *Hukum, Telekomunikasi, Penyiaran, dan Teknologi Informasi Regulasi dan Konvergensi*, (Bandung: PT Revika Aditama, 2013), Halaman 3.

⁹ *Ibid*, Halaman 19.



privasi, sebagaimana diatur dalam *Article 17 International Covenant on Civil and Political Rights*.

1.3. Konvensi Eropa tentang Hak Asasi Tahun 1950 (*European Convention on Human Rights*)

Perlindungan terhadap privasi yang diatur dalam *European Convention on Human Rights* terdapat dalam *Article 8* tentang *Right to respect for private and family life*.

Tanggal 25 November 2014, komite ketiga Majelis Umum PBB (*The Third Committee of the United Nations General Assembly*) mengadopsi resolusi yang menyerukan negara-negara untuk menghormati dan melindungi hak privasi di era digital. Resolusi ini dimotori oleh Jerman dan Brazil. Usulan Jerman dan Brazil diadopsi oleh *The Third Committee of the United Nations General Assembly* dan memutuskan hal-hal diantaranya adalah sebagai berikut:¹⁰

Menyerukan kepada semua negara:

- a. Untuk menghormati dan melindungi hak atas privasi, termasuk dalam konteks komunikasi digital;
- b. Untuk mengambil langkah-langkah untuk mengakhiri pelanggaran hak-hak dan menciptakan kondisi untuk mencegah pelanggaran tersebut, termasuk dengan memastikan bahwa undang-undang nasional yang relevan sesuai dengan

kewajiban mereka di bawah hukum HAM internasional.

- c. Untuk meninjau prosedur, praktik dan undang-undang tentang pengawasan komunikasi, intersepsi, dan pengumpulan data privasi, termasuk pengawasan massa, intersepsi dan pengumpulan mereka, dengan maksud untuk menegakan hak privasi dengan memastikan implementasi penuh dan efektif semua kewajiban mereka di bawah hukum HAM internasional.

Berdasarkan yang telah dijelaskan, dapat diketahui bahwa perlindungan terhadap privasi telah diakui baik secara nasional di Negara Indonesia maupun secara internasional. Sehingga, negara-negara di dunia, termasuk Negara Indonesia memiliki kewajiban untuk melakukan perlindungan atas suatu privasi.

2. Kebijakan Formulasi Terhadap Tindakan Mengakses Informasi Elektronik Secara Ilegal Berdasarkan Hukum Pidana di Indonesia Saat Ini

Saat ini, terdapat beberapa Peraturan Perundang-undangan yang memberikan perlindungan terhadap tindakan mengakses Informasi Elektronik secara ilegal. Lebih jelasnya akan dijabarkan sebagai berikut:

2.1. Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

¹⁰*Ibid*, Halaman 57.



Tindakan mengakses Informasi Elektronik secara ilegal yang diatur dalam Undang-undang Nomor 23 Tahun 2006 terdapat dalam Pasal 79 ayat (1) *jo* Pasal 95 dan Pasal 86 ayat (1) *jo* Pasal 95, yaitu:

Pasal 79 ayat (1)

Data dan dokumen kependudukan wajib disimpan dan dilindungi oleh negara.

Pasal 86 ayat (1)

Menteri sebagai penanggung jawab memberikan hak akses kepada petugas pada Penyelenggara dan Instansi Pelaksana untuk memasukkan, menyimpan, membaca, mengubah, meralat dan menghapus, mengkopi Data serta mencetak Data Pribadi.

Pasal 95

Setiap orang yang tanpa hak mengakses database kependudukan sebagaimana dimaksud dalam Pasal 79 ayat (1) dan/atau Pasal 86 ayat (1) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp. 25.000.000,00 (dua puluh lima juta rupiah).

2.2. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Tindakan mengakses Informasi Elektronik secara ilegal berdasarkan Undang-undang Nomor 36 Tahun 1999 dilakukan dengan cara penyadapan, yaitu terdapat dalam Pasal 40 *jo* Pasal 56, yaitu:

Pasal 40

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

Pasal 56

Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.

2.3. Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

Tindakan mengakses Informasi Elektronik secara ilegal berdasarkan Undang-Undang Nomor 14 Tahun 2008 diatur dalam Pasal 17 huruf a *jo* Pasal 54 ayat (1), Pasal 17 huruf b *jo* Pasal 54 ayat (1), Pasal 17 huruf c *jo* Pasal 54 ayat (2), Pasal 17 huruf d *jo* Pasal 54 ayat (1), Pasal 17 huruf e *jo* Pasal 54 ayat (2), Pasal 17 huruf f *jo* Pasal 54 ayat (1), Pasal 17 huruf g *jo* Pasal 54 ayat (1), Pasal 17 huruf h *jo* Pasal 54 ayat (1), Pasal 17 huruf i *jo* Pasal 54 ayat (1), dan Pasal 17 huruf j *jo* Pasal 54 ayat (1).

Aturan mengenai Tindakan mengakses Informasi Elektronik secara ilegal berdasarkan Undang-Undang Nomor 14 Tahun 2008, lebih jelasnya adalah sebagai berikut:

Pasal 17

Setiap Badan Publik wajib membuka akses bagi setiap Pemohon Informasi Publik



untuk mendapatkan Informasi Publik, kecuali:

a. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat menghambat proses penegakan hukum, yaitu informasi yang dapat:

1. Menghambat proses penyelidikan dan penyidikan suatu tindak pidana;
2. Mengungkapkan identitas informan, pelapor, saksi, dan/atau korban yang mengetahui adanya tindak pidana;
3. Mengungkapkan data intelijen kriminal dan rencana-rencana yang berhubungan dengan pencegahan dan penanganan segala bentuk kejahatan transnasional;
4. Membahayakan keselamatan dan kehidupan penegak hukum dan/atau keluarganya; dan/atau
5. Membahayakan keamanan peralatan, sarana, dan/atau prasarana penegak hukum.

b. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat;

c. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat membahayakan pertahanan dan keamanan negara, yaitu:

1. Informasi tentang strategi, intelijen, operasi, taktik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara, meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri;
2. Dokumen yang memuat tentang strategi, intelijen, operasi, teknik dan taktik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara yang meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi;
3. Jumlah, komposisi, disposisi, atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya;
4. Gambar dan data tentang situasi dan keadaan pangkalan dan/atau instalasi militer;
5. Data perkiraan kemampuan militer dan pertahanan negara lain terbatas pada segala tindakan dan/atau indikasi negara tersebut yang dapat membahayakan kedaulatan negara kesatuan republik indonesia dan/atau data terkait kerjasama militer dengan negara lain yang disepakati dalam



- perjanjian tersebut sebagai rahasia atau sangat rahasia;
6. Sistem persandian negara; dan/atau
 7. Sistem intelijen negara.
- d. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkapkan kekayaan alam Indonesia;
- e. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan ketahanan ekonomi nasional:
1. Rencana awal pembelian dan penjualan mata uang nasional atau asing, saham dan aset vital milik negara;
 2. Rencana awal perubahan nilai tukar, suku bunga, dan model operasi institusi keuangan;
 3. Rencana awal perubahan suku bunga bank, pinjaman pemerintah, perubahan pajak, tarif, atau pendapatan negara/daerah lainnya;
 4. Rencana awal penjualan atau pembelian tanah atau properti;
 5. Rencana awal investasi asing;
 6. Proses dan hasil pengawasan perbankan, asuransi, atau lembaga keuangan lainnya; dan/atau
 7. Hal-hal yang berkaitan dengan proses pencetakan uang.
- f. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan kepentingan hubungan luar negeri:
1. Posisi, daya tawar dan strategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negosiasi internasional;
 2. Korespondensi diplomatik antarnegara;
 3. Sistem komunikasi dan persandian yang digunakan dalam menjalankan hubungan internasional; dan/atau
 4. Perlindungan dan pengamanan infrastruktur strategis Indonesia di luar negeri.
- g. Informasi Publik yang apabila dibuka dapat mengungkapkan isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang;
- h. Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkap rahasia pribadi, yaitu:
1. Riwayat dan kondisi anggota keluarga;
 2. Riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang;
 3. Kondisi keuangan, aset, pendapatan, dan rekening bank seseorang;
 4. Hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang; dan/atau
 5. Catatan yang menyangkut pribadi seseorang yang



berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.

- i. Memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan;
- j. Informasi yang tidak boleh diungkapkan berdasarkan Undang-Undang.

Pasal 54

- (1) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/ atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf a, huruf b, huruf d, huruf f, huruf g, huruf h, huruf i, dan huruf j dipidana dengan pidana penjara paling lama 2 (dua) tahun dan pidana denda paling banyak Rp10.000.000,00 (sepuluh juta rupiah).
- (2) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf c dan huruf e, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp20.000.000,00 (dua puluh juta rupiah).

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

Berdasarkan Undang-undang Nomor 11 Tahun 2008, perbuatan mengakses Informasi Elektronik secara ilegal dapat dilakukan dengan 2 (dua) cara, yaitu dengan cara:

1. Mengakses Komputer dan/atau Sistem Elektronik untuk memperoleh Informasi Elektronik.
2. Melakukan Intersepsi atau penyadapan Informasi Elektronik.

Untuk lebih jelasnya, akan dijelaskan sebagai berikut:

a. Mengakses Komputer dan/atau Sistem Elektronik untuk Memperoleh Informasi Elektronik

Perbuatan mengakses Komputer dan/atau Sistem Elektronik dengan tujuan memperoleh Informasi Elektronik secara ilegal diatur dalam Pasal 30 ayat (2) *jo* Pasal 46 ayat (2) Undang-undang Nomor 11 Tahun 2008, yaitu sebagai berikut:

Pasal 30 ayat (2)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Pasal 46 ayat (2)

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau



denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

b. Melakukan Intersepsi atau Penyadapan Informasi Elektronik

Tindakan intersepsi atau penyadapan dikategorikan sebagai tindak pidana, sebagaimana diatur dalam Pasal 31 ayat (1) dan ayat (2) *jo* Pasal 47 Undang-undang Nomor 11 Tahun 2008, yaitu:

Pasal 31 ayat (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.

Pasal 31 ayat (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.

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Sebagaimana yang telah dijelaskan, bahwa intersepsi atau penyadapan merupakan suatu tindak pidana. Namun, terdapat intersepsi atau penyadapan yang diperbolehkan oleh hukum (tidak bertentangan dengan Peraturan Perundang-undangan). Intersepsi atau penyadapan yang dimaksud yaitu intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya.

Berdasarkan Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010, maka regulasi tentang tata cara penyadapan hanya dapat dilakukan dengan Undang-undang.

Demikianlah penjabaran mengenai kebijakan formulasi terhadap tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum pidana di Indonesia saat ini.

B. Kebijakan Formulasi Terhadap Tindakan Mengakses Informasi Elektronik Secara Ilegal Berdasarkan Hukum Pidana di Indonesia Yang Akan Datang

Kebijakan formulasi tentang tindakan mengakses Informasi



Elektronik secara ilegal berdasarkan hukum pidana di Indonesia yang lebih baik di masa yang akan datang. Lebih jelasnya akan dijabarkan sebagai berikut:

B.1. Tindakan mengakses Informasi Elektronik secara Ilegal dalam Rancangan Kitab Undang-undang Hukum Pidana¹¹

Rancangan Kitab Undang-undang Hukum Pidana (KUHP) memberikan pengaturan terhadap tindakan mengakses Informasi Elektronik secara ilegal di beberapa pasal, yaitu:

a. Tentang Penyadapan

Diatur dalam Pasal 300, Pasal 301, dan Pasal 302.

b. Tentang Penggunaan dan Perusakan Informasi Elektronik dan Domain

Diatur dalam Pasal 373

c. Tentang Tanpa Hak Mengakses Komputer dan Sistem Elektronik

Diatur dalam Pasal 376 huruf a, Pasal 376 huruf c, Pasal 377, dan Pasal 378 huruf a.

Selain mengatur mengenai tindak pidana, Rancangan KUHP juga mengatur masalah percobaan, penyertaan, dan pengulangan melakukan tindak pidana, termasuk terhadap tindakan mengakses Informasi Elektronik secara Ilegal. Hal tersebut diatur dalam Pasal 17

sampai Pasal 20 untuk percobaan, Pasal 21 sampai Pasal 23 untuk penyertaan, dan Pasal 24 untuk pengulangan.

B.2. Peraturan tentang tindakan mengakses Informasi Elektronik secara ilegal di beberapa negara

B.2.1. SINGAPURA

Menurut *Computer Misuse Act (Of Singapore)*, tindakan mengakses Informasi Elektronik secara ilegal merupakan suatu tindak pidana. Hal tersebut sebagaimana diatur dalam Bagian 2 mengenai Tindak Pidana, Pasal 3, Pasal 4, dan Pasal 6 *Computer Misuse Act (Of Singapore)*.

Selain mengatur bahwa mengakses Informasi Elektronik secara ilegal merupakan suatu tindak pidana, *Computer Misuse Act (Of Singapore)* juga mengatur tentang percobaan dan penyertaan melakukan tindak pidana, termasuk percobaan dan penyertaan melakukan tindakan mengakses Informasi Elektronik secara ilegal. Hal tersebut diatur dalam Pasal 10 *Computer Misuse Act (Of Singapore)*.

B.2.2. FILIPINA

Tindakan mengakses Informasi Elektronik secara ilegal, berdasarkan peraturan di Negara Filipina, diatur dalam *Cybercrime Prevention Act 2012*. Hal tersebut diatur dalam Bagian 4 (a) ayat (1) *jo* Bagian 8 dan

¹¹Rancangan KUHP Nasional Indonesia Tahun 2012.



Bagian 4 (a) ayat (2) *jo* Bagian 8 *Cybercrime Prevention Act 2012*.

Selain mengatur mengenai tindak pidana sebagaimana yang telah dijelaskan, *Cybercrime Prevention Act 2012* juga mengatur masalah percobaan dan penyertaan melakukan tindak pidana. Hal tersebut diatur dalam Bagian 5 (a) dan (b) *Cybercrime Prevention Act 2012*.

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, maka diperoleh kesimpulan:

1. Kebijakan formulasi terhadap tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum pidana di Indonesia saat ini diatur dalam Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, dan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Peraturan Perundang-undangan tersebut mengatur bahwa tindakan mengakses Informasi Elektronik secara ilegal dirumuskan sebagai suatu tindak pidana.
2. Kebijakan formulasi terhadap tindakan mengakses Informasi Elektronik secara ilegal berdasarkan hukum pidana di Indonesia yang akan datang sudah mulai diatur melalui

Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012. Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012 memiliki aturan yang melengkapi hal-hal yang belum diatur dalam Peraturan Perundang-undangan di Indonesia mengenai tindakan mengakses Informasi Elektronik secara ilegal saat ini. Selain dalam Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012, Negara Singapura dan Negara Filipina juga memiliki aturan yang mengatur hal-hal yang lebih lengkap dibandingkan dengan Peraturan Perundang-undangan di Indonesia tentang tindakan mengakses Informasi Elektronik secara ilegal saat ini. Hal tersebut diantaranya aturan mengenai “percobaan melakukan tindak pidana”, “penyertaan dalam melakukan tindak pidana”, dan “pengulangan dalam melakukan tindak pidana” yang dapat diterapkan untuk tindakan mengakses Informasi Elektronik secara ilegal.

Berdasarkan hasil penelitian dan pembahasan, maka disarankan:

1. Untuk memberikan dasar pijakan yang kuat dalam upaya pencegahan dan penindakan atas tindakan mengakses Informasi Elektronik secara ilegal, serta memudahkan dalam pelaksanaan perlindungan terhadap korban, maka disarankan bagi Dewan Perwakilan Rakyat untuk segera



melakukan sidang paripurna atas Rancangan Kitab Undang-undang Hukum Pidana Indonesia, dan segera memberlakukan Kitab Undang-undang Hukum Pidana Indonesia yang telah diparipurnakan tersebut.

2. Melihat banyaknya aturan mengenai penyadapan, baik penyadapan yang merupakan suatu tindak pidana, maupun penyadapan yang bukan merupakan suatu tindak pidana di berbagai Peraturan Perundang-undangan di Indonesia. Maka disarankan bagi Dewan Perwakilan Rakyat bersama Pemerintah untuk membuat satu aturan hukum yang khusus mengatur mengenai penyadapan. Sehingga, hal-hal mengenai penyadapan dapat diatur lebih komprehensif dan sistematis dalam satu Peraturan-undangan yang khusus mengatur penyadapan.
3. Disarankan kepada Dewan Perwakilan Rakyat bersama Pemerintah serta seluruh praktisi hukum di Indonesia, termasuk para akademisi untuk selalu memperhatikan nilai-nilai yang hidup di dalam masyarakat Indonesia dalam melakukan pembaharuan hukum pidana. Pembaharuan hukum pidana juga tidak boleh bertentangan dengan Pancasila dan Undang-undang Dasar Negara Republik Indonesia Tahun 1945.

V. DAFTAR PUSTAKA

Buku Literatur

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Bandung: PT Refika Aditama, 2005).

Ali, Zainuddin, *Metode Penelitian Hukum*, (Jakarta: Sinar Grafika, 2010).

Budhijanto, Danrivanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi Regulasi & Konvergensi*, (Bandung: Revika Aditama, 2013).

Dewi Rosadi, Sinta, *Cyber law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, (Bandung: PT Refika Aditama, 2015).

Hanitjo Soemitro, Ronny, *Metodologi Penelitian Hukum*, (Jakarta: Ghalia Indonesia, 1982).

Hamzah, Andi, *Terminologi Hukum Pidana*, (Jakarta: Sinar Grafika Offset, 2008).

Kementerian Komunikasi dan Informatika Republik Indonesia, *101 Tanya Jawab Seputar UU ITE*, 2013.



- Moeleong, Lexi J, *Metodologi Penelitian Kualitatif (edisi revisi)*, (Bandung: Remaja Rosdakarya Offset, 2005).
- Moeljatno, *Asas-asas Hukum Pidana Edisi Revisi*, (Jakarta: PT Rineka Cipta, 2009).
- Nawawi Arief, Barda, *Perbandingan Hukum Pidana*, (Jakarta: Raja Grafindo Persada, 2014).
-, *Tindak Pidana Mayantara Perkembangan Kajian Cyber di Indonesia*, (Jakarta : Raja Grafindo Persada, 2006).
-, *Bunga Rampai Kebijakan Hukum Pidana*, (Bandung: Citra Aditya Bakti, 2005).
-, *Kapita Selekta Hukum Pidana*, (Bandung: Citra Aditya Bakti, 2013).
-, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, (Yogyakarta: Genta Publishing, 2010).
- Prasetyo, Teguh, *Kriminalisasi Dalam Hukum Pidana*, (Bandung: Nusa Media, 2013).
- Serikat Putra Jaya, Nyoman, *Hukum dan Hukum Pidana di Bidang Ekonomi*, (Semarang: Badan Penerbit Universitas Diponegoro, 2014).
- Sudarto, *Hukum Pidana I*, (Semarang: Yayasan Sudarto d/a Fakultas Hukum Undip Semarang, 1990).
- Suhariyanto, Budi, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta: PT Rajagrafindo Persada, 2013).
- Suparni, Ninik, *Cyberspace Problematika Antisipasi Pengaturannya*, (Jakarta: Sinar Grafika, 2009), Halaman 111.
- Soekato, Soerjono, *Pengantar Penelitian Hukum*, (Jakarta: Universitas Indonesia, 1986).
- Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, (Jakarta: Rajawali, 1985).
- Teguh Prasetyo dan Abdul Halim Barkatullah, *Politik Hukum Pidana Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*, (Yogyakarta: Pustaka Pelajar, 2012).



Peraturan Perundang-undangan

Undang-undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-undang Nomor 8 Tahun 1995 tentang Pasar Modal.

Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi.

Undang-Undang Nomor 15 Tahun 2003 tentang Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-Undang.

Undang-undang Nomor 19 Tahun 2003 tentang Badan Usaha Milik Negara.

Undang-undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Surat Keputusan Ketua Mahkamah Agung No. 144/ KMA/ SK/ VIII/ 2007.

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

Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-undang Nomor 35 Tahun

2009 tentang Narkotika.

Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010.

Rancangan Kitab Undang-undang Hukum Pidana Indonesia Tahun 2012.

Deklarasi Universal tentang Hak Asasi Manusia Tahun 1948 (*Universal Declaration of Human Rights*).

Konvensi Eropa tentang Hak Asasi Tahun 1950 (*European Convention on Human Rights*).

Kovenan Internasional tentang Hak-hak Sipil dan Politik Tahun 1966 (*International Covenant on Civil and Political Rights*).

Misuse Act (Of Singapore) Negara Singapura.

Cybercrime Prevention Act 2012 Negara Filipina.

Website

<http://inet.detik.com>

<http://www.lawismayway.blogspot.com>

[http:// www.kbbi.web.id](http://www.kbbi.web.id)

<http://www.hukumonline.com>