POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN *CYBERCRIME*

Dewi Bunga
Fakultas Hukum Universitas Gadjah Mada
Email: bunga8287@gmail.com
Naskah Diterima: 10/02/2019, disetujui 15/03/2019

Abtract

The weaknesses in cyberspace can be a global disaster that threatens the business sector, national and global security, behavior, child protection, and government systems. Cybercrime has been proven to be detrimental to the global community, while efforts to combat cybercrime are still hampered by a variety of factors, therefore, the need for criminal policy against cybercrime eradication. In this research, we will discuss three substances: criminalization of cybercrime in Indonesian legislation, the comparison of criminal policy against cybercrime in some countries, and the strategy in the cybercrime eradication. Criminalization of cybercrime in Indonesian legislation is formulated in the Act on Information and Electronic Transactions. The United States, Britain and Singapore have legislation in combating cybercrime and have a national strategy in handling such crimes. African countries have only temporary legislation and policies with an ad-hoc approach in the fight against cybercrime. Strategies in the eradication of cybercrime are done through penal and non penal policies.

Keywords: *Criminal policy, cybercrime, criminalization.*

Abstrak

Kelemahan dalam ruang maya dapat menjadi bencana global yang mengancam sektor bisnis, keamanan nasional dan global, perilaku, perlindungan anak, dan sistem pemerintahan. *Cybercrime* telah terbukti merugikan komunitas global, sementara upaya untuk memberantas *cybercrime* masih terhambat oleh berbagai faktor, oleh karena itu, diperlukan kebijakan hukum pidana terhadap penanggulangan *cybercrime*. Dalam penelitian ini, kita akan membahas tiga substansi yakni kriminalisasi *cybercrime* dalam perundang-undangan di Indonesia, perbandingan politik hukum pidana terhadap *cybercrime* di beberapa negara, dan strategi dalam pemberantasan cybercrime Kriminalisasi kejahatan dunia maya dalam undang-undang Indonesia dirumuskan dalam Undang-Undang tentang Informasi dan Transaksi Elektronik. Amerika Serikat, Inggris, dan Singapura memiliki undang-undang dalam memerangi kejahatan dunia maya dan memiliki strategi nasional dalam menangani kejahatan semacam itu. Negara-negara Afrika hanya memiliki undang-undang dan kebijakan sementara dengan pendekatan *ad-hoc* dalam memerangi kejahatan dunia maya. Strategi dalam pemberantasan *cybercrime* dilakukan melalui kebijakan pidana dan non pidana.

Kata kunci: *Politik Hukum Pidana, cybercrime, kriminalisasi*

A. Pendahuluan

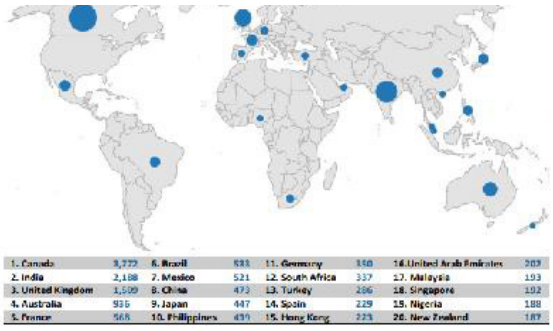
Kemajuan teknologi berimplikasi pada perkembangan kejahatan. Kejahatan-kejahatan tradisional kini bertransformasi menjadi kejahatan di dunia maya (*cybercrime*) dengan menggunakan media internet dan alat-alat elektronik lainnya. Internet memberikan peluang bagi pelaku-pelaku kejahatan di dunia maya untuk melakukan kejahatan dengan lebih rapi, tersembunyi, terorganisasi serta dapat menembus ruang dan waktu dengan jangkauan yang sangat luas. Sebagai salah satu bentuk globalisasi kejahatan, *cybercrime* dapat dilakukan dengan melibatkan beberapa pelaku yang berada di beberapa wilayah yurisdiksi negara yang berbeda dengan target korban yang berada di negara lain pula.

Kejahatan di dunia maya dapat dilakukan tanpa memerlukan kontak antara pelaku dengan korban. Kejahatan dapat dilakukan dimana saja, tanpa memperhitungkan jarak antara pelaku dengan target kejahatan, sepanjang ada jaringan internet dan peralatan yang memadai. Mengenai karakteristik *cybercrime* tersebut Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon[1] mengatakan "*Cyber criminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national. For example, small local networks, as well as groups centred on relatives and friends, remain significant actors.* (Penjahat *cyber* dapat beroperasi sebagai jaringan longgar, namun bukti menunjukkan bahwa anggota masih berada dalam jarak dekat yang dekat bahkan ketika serangan mereka lintas negara. Misalnya, jaringan lokal kecil, serta kelompok yang berpusat pada saudara dan teman, tetap merupakan aktor penting (translasi oleh peneliti)).

UNODC[2], dalam laporannya yang bertajuk "*Comprehensive Study on Cybercrime",* menyatakan "*In the case of computer-related acts causing personal harm, such as the use of a computer system to harass, bully, threaten, stalk or to cause fear or intimidation of an individual, or 'grooming' of a child, the offence object may be regarded as the individual targeted."* Dalam kasus tindakan terkait komputer yang menyebabkan kerusakan pribadi, seperti penggunaan sistem komputer untuk mengganggu, menggertak, mengancam, menguntit atau menimbulkan ketakutan atau intimidasi terhadap seseorang, atau 'penampilan' anak, objek pelanggaran dapat dilakukan dianggap sebagai target individu.

Kejahatan yang dilakukan di ruang maya pada umumnya bertujuan untuk menghasilkan keuntungan finansial bagi pelakunya. Berbagai tindakan dilakukan untuk menyerang sistem keamanan di dunia maya untuk mendapatkan uang. Adapula pelaku yang menggunakan internet sebagai media untuk menghasilkan uang, misalnya penggunaan internet untuk perdagangan gelap senjata dan organ tubuh, prostitusi dan pornografi. Dalam perkembangannya, pelaku kejahatan menggunakan media internet sebagai sarana untuk menyerang pribadi seseorang tanpa secara langsung atau memang tidak bertujuan untuk keuntungan finansial, misalnya pencemaran nama baik melalui internet, *political hacking, cyberterrorism, cyberbullying* dan sebagainya.

Dalam *FBI's Cybercrime Report 2017*, Kepolisian Amerika Serikat tersebut merilis 20 negara tertinggi yang menjadi korban *cybercrime* selain Amerika Serikat. Data tersebut dapat dilihat pada gambar berikut:



1 Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", International Journal of Cyber Criminology Vol 8 Issue 1 January - June 2014, hal. 3.

2 UNODC, 2013, Comprehensive Study on Cybercrime, United Nations New York, hal. 17.

Statistik 20 Negara yang menjadi korban *cybercrime*[3]

Di AS, negara yang paling rentan dalam kejahatan di dunia maya ini adalah California, New York, dan Florida; sementara Kanada menduduki puncak daftar korban asing yang disurvei di 3.722. India, Inggris, Australia, dan Prancis juga menduduki posisi 5 besar.[4] Kejahatan Internet yang paling banyak dilakukan memiliki kasus non-pembayaran / non-pengiriman di tempat pertama, dengan lebih dari 81.000 insiden yang dilaporkan terjadi dimana orang tidak dibayar untuk layanan mereka atau tidak menerima produk yang mereka pesan.[5]

Indonesia sendiri tidak termasuk dalam deretan teratas dalam daftar negara yang menjadi korban *cybercrime,* namun menjadi negara asal dimana *cybercrime* dilakukan. Lona Olavia[6] melaporkan *"Indonesia has received greater scrutiny from cybercrime authorities in recent years, especially since a 2013 survey by Akamai Technologies, an IT security firm, reported that Indonesia had overtaken China as the number one source of hacking traffic in the world."* Indonesia telah mendapat pengawasan yang lebih besar dari pihak otoritas *cybercrime* beberapa tahun terakhir, terutama sejak survei tahun 2013 oleh Akamai Technologies, sebuah perusahaan keamanan TI, melaporkan bahwa Indonesia telah berhasil mengalahkan China sebagai sumber *hacking traffic* terbesar di dunia (translasi oleh peneliti). Data tersebut tidak semata-mata diartikan bahwa pelaku berasal dari Indonesia, namun ada pelaku Warga Negara Asing yang melakukan kejahatan tersebut di Indonesia dengan menggunakan *server* Indonesia. Hal ini dilakukan karena pelaku melihat celah-celah hukum yang dapat diterobos oleh pelaku untuk terhindar dari jeratan hukum.

Pemberantasan *cybercrime* bukanlah hal yang mudah, hal ini mengingat karaktaristik dari kejahatan itu sendiri. Ada beberapa hal yang menjadi kendala dalam penanggulangan kejahatan ini, antara lain:

a. Belum ada persamaan definisi hukum mengenai *cybercrime,* meskipun dalam tataran terorestis sudah banyak ahli yang mencoba untuk memberikan definisi mengenai *cybercrime.*
b. Formulasi hukum yang ada belum dapat menjangkau perkembangan kejahatan yang dilakukan di dunia maya. Sampai saat ini, Indonesia memang belum memiliki Undang-undang tentang Perlindungan Data Pribadi sebagaimana negara lain. Perlindungan data pribadi sementara ini hanya didasarkan pada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
c. Karakteristik kejahatan di dunia maya menunjukkan bahwa kejahatan ini dapat melintasi yurisdiksi negara, sementara keberadaan perjanjian internasional mengenai penegakan hukum terhadap *cybercrime* masih sangat terbatas.
d. Kebijakan penal dalam penanggulangan *cybercrime* belum diimbangi dengan kebijakan non penal seperti kebijakan dalam lingkungan kerja, kebijakan dalam aplikasi, kebijakan di sekolah dan sebagainya.
e. Penegak hukum harus berhadapan dengan milyaran *netizen* (pengguna internet) dengan perilaku berinternet yang beraneka macam. Sumber daya penegak hukum yang belum memadai menjadi tantangan dalam menanggulangi *cybercrime.*
f. Kurangnya barang bukti dalam pengungkapan kasus. Dalam sejumlah kasus di dunia maya, keejahatan terjadi dalam aplikasi atau media yang dioperasikan di luar negeri, hal ini akan menyulitkan kepolisian untuk meminta bukti

3 Scott S. Smith, 2016, Internet Crime Report, Federal Bureau of Investigation, Internet Crime Complaint Center, Washington D.C., hal. 15.

4 FBI, "FBI's Cybercrime Report 2017", https://www.cybersecurityintelligence.com/blog/fbis-cybercrime-report-2017-2575.html, diakses pada 12 Desember 2018.

5 Ibid.

6 Lona Olavia, "Cybercrime Threat a Growing Concern: Police", http://www.jakartaglobe.beritasatu.com/news/cybercrime-threat-growing-concern-police/, diakses pada 12 Desember 2018.

kepada penyedia. Pihak bank juga menolak untuk memberikan data nasabah, mutasi rekening dan aliran dana sehubungan dengan adanya kewajiban rahasia perbankan.

g. Belum ada batas yang tegas antara hak atas informasi dengan hak kebebasan berekspresi di dunia maya, dimana kedua hak tersebut merupakan hak asasi manusia.

h. Budaya masyarakat yang kurang waspada dalam mencegah dirinya untuk menjadi korban kejahatan di dunia maya, misalnya mudah memberikan identitas pribadi, menggunggah foto dan video yang tidak seharusnya dibagikan, dan mudah mempercayai orang-orang yang baru dikenal di dunia maya.

Kejahatan di dunia maya mengancam sektor bisnis dan kehancuran terhadap perilaku pengguna internet. Dunia maya sering pula dimanfaatkan oleh para ekstrimis untuk memasukkan ideologi-ideologi radikal yang mengancam keutuhan berbangsa dan bernegara. Dalam melakukan penanggulangan terhadap *cybercrime* diperlukan politik hukum pidana. Politik hukum pidana merupakan upaya masyarakat untuk menetapkan hukum dalam rangka mencegah kejahatan.[7] Politik hukum pidana diarahkan pada penanggulangan secara komprehensif dari berbagai bentuk kejahatan di dunia maya.

B. Pembahasan

1. Kriminalisasi *Cybercrime* dalam Perundang-undangan di Indonesia

Kriminalisasi (*criminalization*) merupakan tindakan atau penetapan penguasa mengenai perbuatan-perbuatan tertentu yang oleh masyarakat atau golongan-golongan masyarakat dianggap sebagai perbuatan yang dapat dipidana menjadi perbuatan pidana.[8] Formulasi kejahatan di dunia maya dapat dilihat pada pengaturan tindakan tersebut dalam undang-undang. Dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur sejumlah perbuatan yang dilarang yang menjadi tindakan *cybercrime.* Ketentuan-ketentuan tersebut juga dikaitkan dengan ketentuan dalam KUHP. Tindakan-tindakan *cybercrime* yang diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronikyakni sebagai berikut:

1) Tindakan yang melanggar kesusilaan.

Dalam Pasal 27 ayat (1) Undang-undang Nomor 11 Tahun 2008 dinyatakan ”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 kesusilaan.” Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik sendiri tidak menjelaskan mengenai perbuatan mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. Perbuatan yang melanggar kesusilaan melalui media internet sendiri mengacu pada KUHP. Delik kesusilaan diatur dalam Bab XIV Buku II KUHP. Adapun perbuatan yang tergolong dalam delik kesusilaan adalah sebagai berikut:

1) Kejahatan dengan sengaja melanggar kesusilaan (Pasal 281 KUHP).
2) Pornografi (Pasal 282, 283, 283 bis KUHP).
3) Perzinahan (Pasal 284 KUHP).
4) Perkosaan (Pasal 285 KUHP).
5) Beresetubuh dengan perempuan yang bukan istri dalam keadaan pingsan atau tidak berdata (Pasal 286 KUHP).
6) Bersetubuh dengan anak (Pasal 287 KUHP).
7) Bersetubuh dengan istri yang belum waktunya dikawin (Pasal 288 KUHP).
8) Pencabulan (Pasal 289 KUHP).
9) Pencabulan terhadap seorang yang pingsan atau tidak berdaya (Pasal 290 ayat (1) KUHP).
10) Pencabulan (Pasal 290 KUHP).

7 Ali Zaidan, 2015, Menuju Pembaruan Hukum Pidana, Sinar Grafika, Jakarta, hal. 63.

8 Soekanto, Soerjono, 1981, Kriminologi: Suatu Pengantar, Cetakan Pertama, Ghalia Indonesia, Jakarta, hal. 62.

11) Perbuatan cabul dengan sesama jenis yang belum dewasa (Pasal 292 KUHP).
12) Menggerakkan orang yang belum dewasa untuk berbuat cabul (Pasal 293 KUHP).
13) Pencabulan terhadap orang yang berada di bawah kekuasaanya (Pasal 294 KUHP).
14) Memudahkan pencabulan terhadap orang yang berada di bawah kekuasaanya (Pasal 295 KUHP).
15) Mucikari (Pasal 296 KUHP).

Dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, ada beberapa tindakan yang tergolong dalam Pasal 27 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu *cyber* pornografi dan prostitusi *online*. Tindak pidana ini semakin berat apabila dilakukan terhadap anak. Salah satu permasalahan yang ditimbulkan dari kemajuan teknologi informasi melalui jaringan internet adalah beragamnya situs yang menampilkan adegan pornografi. Seolah-olah sekarang ini, sulit sekali memproteksi jaringan internet dari serbuan pebisnis hiburan yang menjual pornografi.[9]

2) Perjudian

Perjudian *online* diatur dalam Pasal 27 ayat (2) Undang-undang tentang Informasi dan Transaksi Elektronik. Dalam ketentuan tersebut dinyatakan "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) Penghinaan dan/atau pencemaran nama baik

Penghinaan dan/atau pencemaran nama baik di dunia maya diatur sebagai larangan dalam Pasal 27 ayat (3) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan "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." Dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pembuat undang-undang menyetarakan antara penghinaan dengan pencemaran, pada penghinaan sendiri merupakan suatu kelompok perbuatan sedangkan salah satu bentuk penghinaan adalah pencemaran.

Pembuat undang-undang tampaknya ingin mengarahkan perbuatan penghinaan melalui media internet tersebut sebagai pencemaran. Perbuatan penghinaan dan/atau pencemaran diatur dalam Bab XVI Buku II. Kejahatan penghinaan terdiri atas penghinaan umum dan penghinaan khusus. Penghinaan umum yakni dengan objek harga diri dan martabat orang pribadi, termasuk juga pencemaran sedangkan penghinaan khusus adalah penghinaan yang memiliki objek harga diri, kehormatan dan nama baik komunal.[10] Adapun kualifikasi delik penghinaan dalam KUHP adalah sebagai berikut:

1) Penghinaan umum
   a. Pencemaran
   b. Fitnah
   c. Penghinaan ringan
   d. Pengaduan fitnah
   e. Persangkaan palsu
   f. Penghinaan terhadap orang yang sudah meninggal
2) Penghinaan khusus
   a. Penghinaan terhadap Presiden atau Wakil Presiden RI
   b. Penghinaan terhadap Kepala Negara Sahabat dan wakil negara asing di Indonesia
   c. Penghinaan terhadap Kepala Negara Sahabat dan wakil negara asing di Indonesia dengan cara menyiarkan, mempertunjukkan atau menempelkan tulisan atau lukisan.
   d. Penghinaan terhadap Bendera Kebangsaan dan Lambang Negara RI
   e. Penghinaan terhadap Pemerintah RI
   f. Penghinaan terhadap golongan penduduk tertentu
   g. Penghinaan dalam hal yang berhubungan dengan agama

9 Abdul Wahid dan Mohammad Labib, 2005, Kejahatan Mayantara (Cyber Crime), Refika Aditama, Bandung, hal.146.
10 Adami Chazawi, 2013, Hukum Pidana Positif Penghinaan (Edisi Revisi), Media Nusa Creative, Malang, hal. 81.

h. Penghinaan terhadap penguasa dan badan umum.

Tindakan penghinaan dan/atau pencemaran dapat ditemukan dalam berbagai kolom komentar di dunia maya, terutama ketika korban memindai status, foto, atau video pribadinya. Pelaku juga dapat menuliskan kata-kata yang mengandung penghinaan dan/atau pencemaran pada dinding akunnya, baik dengan atau menautkan pernyataan tersebut kepada korban.

4) Pemerasan dan/atau pengancaman.

Pemerasan dan/atau pengancaman di dunia maya dilarang dalam Pasal 27 ayat (4) Undang-undang Nomor 11 Tahun 2008 yang menyatakan "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." Kualifikasi perbuatan yang tergolong pemerasan dan/atau pengancaman dalam Pasal 368 ayat (1) KUHP menyatakan:

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya membuat hutang maupun menghapuskan piutang, diancam karena pemerasan, dengan pidana penjara paling lama sembilan tahun.

Dalam Pasal 369 KUHP dinyatakan pula sebagai berikut:

(1) Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. dengan ancaman pencemaran baik dengan lisan maupun tulisan, atau dengan ancaman akan membuka rahasia, memaksa seorang supaya memberikan barang sesuatu yang seluruhnya atau sebagian kepunyaan orang itu atau orang lain. atau supaya membuat hutang atau menghapuskan piutang, diancam dengan pidana penjara paling lama empat tahun.

(2) Kejahatan ini tidak dituntut kecuali atas pengaduan orang yang terkena kejahatan.

Kejahatan ini dapat dilakukan ketika pelaku memaksa korban melalui dunia maya untuk memberikan suatu barang yang jika tidak, pelaku akan melakukan tindakan tertentu kepada korban.

5) Penguntitan/*Cyberstalking*

Pasal 29 Undang-undang Nomor 11 Tahun 2008 menyatakan "Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi." Ketentuan dalam Pasal 29 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mirip dengan pengaturan *cyberstalking* di Amerika Serikat, Kanada, Inggis dan negara lainnya. Dalam ketentuan di negara-negara tersebut diatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan rasa takut, baik dengan kata-kata maupun tindakan tertentu. Perbuatan tersebut dilakukan dengan menggunakan atau melalui teknologi informasi dan komukasi, misalnya dengan *unsolicited hate mail, obsence or threatening email, mail bombs* dan lain-lain.[11]

6) Penyebaran berita bohong (*hoax*)

Penyebaran berita bohong diatur dalam Pasal 28 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

7) Ujaran kebencian

Kejahatan ini diatur dalam Pasal 28 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan "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). "Kejahatan sebagaimana diatur dalam Pasal 28 ayat (2) ini juga disebut dengan *hate site.*

11 Sigid Suseno, 2012, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung, hal. 177-178.

8) Akses ilegal

Dalam Pasal 30 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur 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.

9) Intersepsi

Intersepsi diatur dalam Pasal 31 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur mengenai intersepsi. Adapun perbuatan yang tergolong intersepsi sebagaimana dimaksud dalam Pasal 31 adalah sebagai berikut:

(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) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.
(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang."

Dalam Penjelasan Pasal 31 ayat (1) Undang-undang Nomor 19 Tahun 2016 dinyatakan yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

10) Kejahatan terhadap Informasi Elektronik dan/atau Dokumen Elektronik atau *Data interference.*

Kejahatan ini menjadikan Informasi Elektronik dan/atau Dokumen Elektronik sebagai sasaran dalam melakukan kejahatan. Dalam Pasal 32 dinyatakan sebagai berikut:

(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.

11) Gangguan terhadap sistem elektronik

Gangguan terhadap sistem elektronik atau *system interference* adalah kejahatan yang dilakukan dengan

menyerang sistem sebagaimana diatur dalam Pasal 33 yang menyatakan "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."

12) Penyalahgunaan perangkat

Penyalahgunaan perangkat atau *misuse of devices* merupakan tindakan melawan hukum sebagaimana diatur dalam Pasal 34 yaitu:

(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.

13) Pelanggaran yang terkait dengan komputer

Computer-related offences atau pelanggaran terkait komputer biasanya digunakan untuk melakukan pemalsuan (*forgery*) dan penipuan (*fraud*). Dalam Pasal 35 dinyatakan "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."

Formulasi perbuatan dalam peraturan perundang-undangan menjadi landasan dalam melakukan kebijakan penegakan hukum.

2. Perbandingan Politik Hukum Pidana terhadap *Cybercrime* di Beberapa Negara

Kebijakan kriminal digunakan sebagai salah satu alternatif dalam menyelesaikan kebijakan sosial. Penanggulangan masalah sosial dilakukan dengan penegakan hukum yang menjadi respon atas kejahatan yang dilakukan oleh masyarakat. Sebagai suatu respon atas kejahatan, kebijakan kriminal tersebut memiliki keterbatasan dalam menanggulangi kejahatan yang demikian luas dan kompleks, oleh sebab itu penanggulangan kejahatan dilakukan dengan sarana penal (penggunaan hukum pidana) dan diimbangi dengan sarana non penal.[12]

Cybercrime bukan hanya merupakan kejahatan yang harus dihadapi oleh Indonesia saja, melainkan juga negara lain. *Development and implementation of relevant legislations are principal measures in the management of the growing incidences of cybercrime.*[13]

1) Amerika Serikat

Peraturan tentang larangan *cybercrime* dalam hukum Amerika Serikat diatur dalam banyak undang-undang. Amerika serikat membangun regulasi di bidang kejahatan dunia maya dengan mengeluarkan sejumlah peraturan yakni *Acces Device Fruade Act of 1984, Computer Fraud and Abuse Act of 1986, Transportation of Obsence Matters for Sale or Distribution, National Infrastructure Protection Act of 1996, Communication Decency Act of 1996, the Cyberspace Electronic Security Act of 1999,"* dan *the "Patriot Act of 2001* dan sebagainya.

Ditinjau dari sisi praktik penegakan hukum, investigasi dilakukan oleh FBI dengan bekerjasama dengan jejaring. FBI bekerjasama dengan of the *Internet Crime Complaint Center* (IC3). Dalam laman resmi FBI[14] disebutkan:

12 Barda Nawawi Arief, 2005, Pembaharuan Hukum Pidana; Dalam Perpekstif Kajian Perbandingan, Citra Aditya Bakti, Bandung, hal. 102.

13 Corlane Barclay, "Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM)", Information Technology for Development, 2014 Vol. 20, No. 2, 165–195, hal. 165.

14 FBI, "Cyber Crime", https://www.fbi.gov/investigate/cyber, diakses pada 12 Desember 2018.

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Misi dari *the Internet Crime Complaint Center (IC3*) adalah menyediakan mekanisme pelaporan yang andal dan nyaman kepada publik untuk menyampaikan informasi kepada FBI terkait dugaan skema penipuan yang difasilitasi Internet dan untuk mengembangkan aliansi yang efektif dengan para penegak hukum dan mitra industri. Informasi dianalisis dan disebarluaskan untuk tujuan investigasi dan intelijen untuk penegakan hukum dan untuk kesadaran masyarakat (translasi oleh peneliti).

Amerika Serikat juga memiliki *Cyber Action Team* yang bertugas untuk untuk memberikan respon yang cepat terhadap gangguan komputer dan keadaan darurat di ruang virtual Mereka adalah agen khusus atau ilmuwan komputer, dan semuanya memiliki pelatihan lanjutan dalam bahasa komputer, penyelidikan forensik, dan analisis perangkat lunak. Tim lain yang juga disiapkan adalah *National Cyber Forensics and Training Alliance* organisasi ini dibentuk pada tahun 1997 dan berbasis di Pittsburgh. *National Cyber Forensics and Training Alliance* telah menjadi model internasional untuk menyatukan penegak hukum, industri swasta, dan akademisi untuk membangun dan berbagi sumber daya, informasi strategis, dan mengancam intelijen untuk mengidentifikasi dan menghentikan ancaman *cyber* yang muncul dan mengurangi ancaman yang ada.[15]

2) Inggris

a. Parlemen Inggris telah mengeluarkan *Data Protection Act of 1984 and the Computer Misuse Act of 1990.* Dalam melakukan penanggulangan terhadap *cybercrime Secretary of State for the Home Department*[16] telah mengeluarkan kebijakan berupa:

b. Coordinate activity across Government to tackle crime and address security on the internet in line with the strategic objectives laid out in the UK Cyber Security Strategy.

c. *Reduce the direct harms by making the internet a hostile environment for financial criminals and child sexual predators, and ensuring that they are unable to operate effectively through work to disrupt crime and prosecute offenders.*

d. *Raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on the threats.*

e. *Support industry leadership to tackle cyber crime, and work with industry to consider how products and online services can be made safer and security products easy to use.*

f. *Work with international partners to tackle the problem collectively.*

g. Mengkoordinasikan kegiatan di seluruh Pemerintah untuk mengatasi kejahatan dan mengatasi keamanan di internet sesuai dengan tujuan strategis yang ditetapkan dalam *UK Cyber Security Strategy*.

h. Mengurangi kerugian langsung dengan membuat internet menjadi lingkungan yang tidak bersahabat bagi penjahat keuangan dan predator seksual anak, dan memastikan bahwa mereka tidak dapat beroperasi secara efektif melalui pekerjaan untuk mengganggu kejahatan dan melakukan penuntutan terhadap pelaku.

i. Meningkatkan kepercayaan publik akan keamanan dan keamanan internet, tidak hanya melalui penanganan kejahatan dan penyalahgunaan, namun melalui penyediaan informasi yang akurat dan mudah dipahami kepada publik mengenai ancaman tersebut.

j. Mendukung kepemimpinan industri untuk mengatasi kejahatan di dunia maya, dan bekerja sama dengan industri untuk mempertimbangkan bagaimana produk dan layanan *online* dapat dibuat lebih aman dan produk keamanan mudah digunakan.

15 Ibid.

16 Secretary of State for the Home Department, 2010, Cyber Crime Strategy, The Stationery Office Limited, London, hal. 17.

k. Bekerjalah dengan mitra internasional untuk mengatasi masalah secara kolektif. (translasi oleh peneliti).

3) Singapura

Ketentuan mengenai *cybercrime* di Singapura diatur dalam *The Computer Misuse Act.* Dalam undang-undang tersebut ada beberapa kategori tindak pidana yakni:

a. Unauthorised access to computer material
b. Access with intent to commit or facilitate commission of offence
c. Unauthorised modification of computer material
d. Unauthorised use or interception of computer service
e. Unauthorised obstruction of use of computer
f. Unauthorised disclosure of access code

a. Akses tidak sah ke materi komputer
b. Akses dengan niat untuk melakukan atau memfasilitasi pelaksanaan tindak pidana
c. Modifikasi materi komputer yang tidak sah
d. Penggunaan atau penyadapan layanan komputer yang tidak sah
e. Gangguan yang tidak sah dalam penggunaan komputer
f. Pengungkapan kode akses yang tidak sah

Pemerintah Singapura melalui *Ministry of Home Affairs*[17] memiliki stratetgi dalam memerangi *cybercrime* yang dapat dikelompokkan ke dalam empat bidang prioritas yakni *educating and empowering the public to stay safe in cyberspace* (mendidik dan memberdayakan masyarakat agar tetap aman di dunia maya), *enhancing the Government's capacity and capability to combat cybercrime* (meningkatkan kapasitas dan kemampuan Pemerintah dalam memerangi kejahatan dunia maya), *strengthening legislation and the criminal justice framework* (memperkuat legislasi dan kerangka peradilan pidana) dan *stepping up partnerships and international engagement* (meningkatkan kemitraan dan keterlibatan internasional).

Amerika Serikat, Inggris dan Singapura, termasuk Indonesia merupakan negara-negara yang telah cukup mapan dalam merancang strategi penanggulangan *cybercrime,* khususnya dalam bentuk formulasi undang-undang. Sebaliknya, sebagian besar negara di kawasan ini, termasuk Burkina Faso, Gambia, Ghana, Kenya, Senegal, dan Zimbabwe menggunakan undang-undang darurat dan dan kebijakan dengan pendekatan *ad hoc* terhadap fenomena *cybercrime.* Negara-negara lain di kawasan ini berusaha mencegah kegiatan tersebut dengan cara memblokir akses ke situs web tertentu.[18]

Kebijakan penanggulangan *cybercrime* di berbagai negara membutuhkan kerjasama internasional, sebab masalah ini menjadi masalah bersama yang dihadapi seiring dengan globalisasi. Murdoch Watney mengatakan "*Cybercrime regulation cannot be separated from global politics. There is no superpower nation-state whose guidance other states will automatically follow.*"[19] (Peraturan *cybercrime* tak lepas dari politik global. Tidak ada negara negara adikuasa yang menjadi panduan negara lainnya untuk secara otomatis akan mengikuti (translasi oleh peneliti)).

3. Strategi dalam Pemberantasan *Cybercrime*

Cybercrime adalah salah satu produk dari globalisasi kejahatan, dimana kejahatan dilakukan tanpa terbatas pada ruang dan waktu. Muladi dan Diah Sulistyani R.S.[20] menjelaskan bahwa akselarasi transportasi, komunikasi dan informasi modern melahirkan globalisasi teknologi yang berpengaruh terhadap globalisasi kejahatan (*globalization of crime*). Lebih lanjut dikatakan, kebijakan hukum pidana (*criminal policy*) yang dapat dilakukan dalam menanggulangi hal tersebut adalah dengan *warmaking criminology or harm creating on crime*

17 Ministry of Home Affairs, "National Cybercrime Action Plan", https://www.mha.gov.sg/Newsroom/press-releases/PublishingImages/Pages/Launch-of-the-, diakses pada 12 Desember 2017. National-Cybercrime-Action-Plan-at-RSA-Conference-Asia-Pacific-Japan/NCAP%20Document.pdf, diakses pada 12 Desember 2018.

18 Dejo Olowu, "Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa", Journal of Information, Law & Technology, 1, 2009, hal. 8.

19 Murdoch Watney, "Cybercrime regulation at a cross-road: state and transnational laws versus global laws" International Conference on Information Society (i-Society 2012) hal. 73.

20 Muladi dan Diah Sulistyani R.S., 2016, Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal, Alumni, Bandung, hal. 24.

yang bersifat bermusuhan (*adversarialism*) sebagai pendekatan represif dan dikombinasikan dengan pendekatan preventif mutualisme atau kebersamaan atas dasar *peacemaking criminology*.[21]

Dalam menanggulangi *cybercrime* maka diperlukan upaya komprehensif baik melalui hukum pidana maupun melalui saluran hukum pidana. Pencegahan dan penanggulangan kejahatan dilakukan dengan pendekatan integral antara kebijakan penal dengan kebijakan non penal. Kebijakan penal memiliki beberapa keterbatasan dan kelemahan yakni bersifar fragmatis, individualitik (*offender oriented*), lebih bersifat represif dan harus didukung dengan infratruktur yang memerlukan biaya tinggi. Dengan demikian maka penanggulangan kejahatan lebih baik dilakukan dengan menggunakan kebijakan non penal yang bersifat preventif.[22] Kebijakan dalam penanggulangan *cybercrime* dapat dilakukan dengan dua acara yakni:

a. Kebijakan penal.
b. Kebijakan non penal.

Kebijakan penal adalah kebijakan yang terkait dengan penggunaan sanksi pidana dalam penyelesaian kasus kejahatan di dunia maya. Kebijakan penal dapat dilakukan melalui cara-cara berikut:

a. Kriminalisasi perbuatan dalam undang-undang sehingga perbuatan tersebut termasuk kejahatan di dunia maya.

   Negara hukum pada pokoknya menentukan bahwa peraturan hukum menjamin tertib negara dan tertib masyarakat.[23] Indonesia adalah negara hukum, sehingga penjatuhan sanksi hukum harus didahului dengan kriminalisasi suatu perbuatan sehingga dapat digolongkan sebagai tindak pidana. Kriminalisasi dapat terjadi karena perkembangan masyarakat yang didukung dengan kemajuan ilmu dan teknologi.[24] Kriminalisasi perlu dilakukan dengan mempertimbangkan kepentingan hukum yang dilindungi supaya tidak terjadi *over* kriminalisasi. Kriminalisasi memang memungkinkan kekacauan dalam struktur hukum telematika. Secara tegas Jonathan Mayer[25] mengatakan sebagai berikut:

   The structure of cybercrime law generates the potential for two different types of redundancy. First, a cybercrime offense might be internally redundant, overlapping with other cybercrime offenses within the same statutory scheme. Second, a cybercrime offense might be externally redundant, overlapping with noncybercrime civil claims or criminal charges.

   Dalam memformulasikan suatu tindakan perlu digolongkan sebagai tindak pidana atau tidak, maka pembuat undang-undang memerlukan batasan antara perlindungan pribadi di satu sisi dan kebebasan berekspresi di sisi lain. Zubair Kasuri, Flare[26] mengatakan "*Civil and human rights activists contend that the law would put unnecessary curbs on freedom of expression on the internet. According to them, it will give undeterred powers to the law-enforcement and investigation authorities to harass innocent people in the name of national security*." Aktivis sipil dan hak asasi manusia berpendapat bahwa undang-undang akan melarang pembatasan kebebasan berekspresi di internet. Menurut mereka, hal itu akan memberi kekuasaan yang tidak berdasar kepada otoritas penegakan hukum dan investigasi untuk melecehkan orang-orang yang tidak bersalah atas nama keamanan nasional (translasi oleh peneliti).

   Indonesia sampai saat ini belum memiliki undang-undang tentang perlindungan data pribadi. Ketentuan mengenai data pribadi memang secara sekilas diatur dalam Pasal 26 Undang-undang Nomor 19 Tahun 2016. Ketentuan terebut belum cukup untuk melindungi penyebaran data pribadi yang sangat

21 Ibid., hal. 24.

22 Hatta, 2010, Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan, Pustaka Pelajar, Yogyakarta, hal. 39.

23 Sri Widoyati Wiratmo Soekito, 1983, Anak dan Wanita dalam Hukum, LP3ES, Jakarta, hal. 85.

24 Andi Hamzah, 1987, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta, hal. 28.

25 Jonathan Mayer, "Cybercrime Litigation", University of Pennsylvania Law Review, Vol. 164, 2016, hal. 1485-1486.

26 Zubair Kasuri, Karachi Flare, "Cybercrime Prevention Law Takes Effect", Karachi Vol. 12, Iss. 11, (Aug 2016), hal. 28.

rentan terjadi di dunia maya. Pornografi anak juga belum menjadi ketentuan yang berdiri sendiri. Tindak pidana ini hanya diancam dengan pidana yang diperberat dibandingkan apabila melibatkan orang dewasa.

b. Harmonisasi ketentuan hukum nasional dengan hukum internasional dalam memberantas *cybercrime*.

Sigid Suseno[27] menggambarkan telah terjadi pendekatan antara pendekatan global dan pendekatan evolusioner yang melahirkan pendekatan kompromistis yakni yang sesuai dengan karakteristik dan kategorisasi *cybercrime.* Pendekatan evolusioner dilakukan dengan mengamandemen rumusan tidak pidana, baik objek maupun cara-cara dilakukannya tindak pidana terhadap *computer related offences* dari tindak pidana tradisional yang terdapat dalam KUHP dan yang diatur dalam Undang-undang khusus di luar KUHP. Pendekatan global dilakukan terhadap *confidentiality integrity,* dan *availability* data komputer atau sistem komputer atau sistem elektronik dengan membentuk pengaturan yang baru dalam Undang-undang khusus.

Badan Pembinaan Hukum Nasional (BPHN)[28] dalam laporan akhir mengenai "Kajian *EU Convention on Cybercrime* dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi" menyatakan bahwa dalam penyusunan regulasi di bidang *cybercrime*, Indonesia memiliki beberapa alternatif strategi yang dapat dilakukan, yaitu dengan:

a) Mengembangkan hukum pidana melalui penyusunan norma-norma hukum positif yang dapat menjangkau kejahatan-kejahatan di bidang teknologi informasi.
b) Mengadopsi prinsip-prinsip regulasi *cybercrime* yang bersifat global dari suatu model norma-norma hukum internasional ke dalam suatu regulasi nasional.
c) Meratifikasi atau mengakses *EU Convention on Cybercrime* 2001 di *Budapest*, dan kemudian menyusun regulasi dan peraturan implementasinya *(implementing legislation*) dalam tataran hukum nasional.

c. Penegakan hukum melalui penjatuhan sanksi pidana bagi pelaku *cybercrime.*

Dalam hukum modern, penggunaan hukum sebagai sarana rekayasa masyarakat (*law as a tool of social engineering*) dilakukan dengan melibatkan para pembuat hukum dengan merumuskan sanksi sebagai sarana penegakan hukum. Penegakan hukum tersebut dilakukan untuk mewujudkan perubahan yang efektif di dalam masyarakat.[29] Penegakan hukum dilakukan untuk memenuhi nilai keadilan, terutama bagi korban. Nilai keadilan menduduki elemen vital dan esensial dalam pembentukan, penerapan dan penegakan hukum. Nilai keadilan tersebut menjadi syarat mutlak dalam kehidupan bermasyarakat, berbangsa dan bernegara sesuai dengan cita hukum Pancasila.[30]

Formulasi hukum telematika sampai saat ini memang belum mencapai tingkat kemapanan. Hal ini disebabkan karena bidang ini mengandung unsur-unsur yang kompleks. Mengenai hal tersebut Marco Gercke[31] mengemukakan sebagai berikut:

Introducing cybercrime legislation is not an easy task as there are various areas that require regulation. In addition to substantive criminal law and procedural law, cybercrime legislation may include issues related to international cooperation, electronic evidence and the liability of an Internet Service Provider (ISP). In most countries elements

27 Sigid Susone, op.cit., hal. 198.

28 Badan Pembinaan Hukum Nasional (BPHN), 2009, "Kajian EU Convention on Cybercrime dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi", Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, Jakarta, hal. 7.

29 Suteki, 2013, Hukum dan Alih Teknologi; Sebuah Pergulatan Sosiologis, Thafa Media, Yogyakarta, hal. 19.

30 Soejadi, 2017, Refleksi Mengenai hukum dan Keadilan;; Aktualisasinya di Indonesia, Aswaja Pressindo, Yogyakarta, hal. 56-57.

31 Marco Gercke, 2012, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU Telecommunication Development Bureau, hal. 100.

of such legislation may already exist – often in different legal frameworks. Provisions related to cybercrime do not necessarily need to be implemented in one single piece of legislation. With regard to existing structures, it might be necessary to update different pieces of legislation (such as amending an Evidence Act to ensure that it is applicable with regard to the admissibility of electronic evidence in criminal proceedings) or remove provision from an older law (for example in a Telecommunications Act) within the process of introducing new legislation.

Memperkenalkan peraturan *cybercrime* bukanlah tugas yang mudah karena ada berbagai area yang memerlukan regulasi. Selain hukum pidana dan hukum acara yang substantif, undang-undang *cybercrime* mungkin mencakup masalah yang berkaitan dengan kerja sama internasional, bukti elektronik dan pertanggungjawaban Penyedia Layanan Internet (ISP). Di sebagian besar negara, unsur-unsur perundang-undangan semacam itu mungkin sudah ada - seringkali dalam kerangka hukum yang berbeda. Ketentuan terkait kejahatan dunia maya tidak perlu diimplementasikan dalam satu undang-undang tunggal. Sehubungan dengan struktur yang ada, mungkin perlu memperbarui bagian undang-undang yang berbeda (seperti mengubah Undang-Undang Bukti untuk memastikan hal itu dapat diterapkan sehubungan dengan diterimanya bukti elektronik dalam proses pidana) atau menghapus ketentuan dari undang-undang yang lebih lawas (untuk contoh dalam Undang-Undang Telekomunikasi) dalam proses memperkenalkan undang-undang baru (translasi oleh peneliti).

Politik hukum pidana dalam penanggulangan *cybercrime* melalui sarana penal perlu diimbangi denggan kebijakan non penal. Kebijakan non penal yang dapat dilakukan adalah sebagai berikut:

a. Menyusun kebijakan di luar hukum pidana yang mendukung upaya pencegahan *cybercrime,* seperti melalui kebijakan anti-kebencian, kebijakan anti-*bullying* dan kebijakan berinternet sehat melalui sistem pendidikan.
b. Melakukan sosialisasi terhadap potensi kejahatan di dunia maya dengan mengedukasi masyarakat pengguna internet untuk tidak mencantumkan identitas pribadi, bertransaksi di tempat dengan fasilitas internet yang aman dan sebagainya.
c. Membangun kerjasama dengan pihak swasta untuk membangun sistem keamanan di dunia maya.
d. Membentuk jaringan kelembagaan dalam mencegah *cybercrime* baik dalam tataran nasional maupun dalam tingkat internasional. Kerjasama internasional dalam penanggulangan *cybercrime* sangat diperlukan mengingat *cybercrime* merupakan kejahatan transnasional yang terorganisir.

Sebagai negara berkembang, Indonesia harus sigap dalam menyesuaikan diri terhadap perkembangan hukum dan strategi dalam penanggulangan kejahatan di dunia maya. Politik hukum dalam menanggulangi *cybercrime* dilakukan dengan menyusun strategi global dalam pencegahan dan penegakan hukum terhadap kejahatan di dunia maya, menyusun formulasi hukum yang responsive dan menyiapkan kelembagaan yang dapat melakukan tindakan cepat ketika terjadi masalah di dunia maya.

C. Penutup

Kriminalisasi *cybercrime* dalam perundang-undangan di Indonesia diformulasikan dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Amerika Serikat, Inggris dan Singapura memiliki undang-undang dalam memberantas *cybercrime* dan memiliki strategi nasional dalam penanggulangan kejahatan tersebut baik dengan membangun kerjasama internasional, membangun kelembagaan yang mapan, mengajak pihak swasta untuk mengembangkan sistem keamanan di dunia maya dan mengedukasi masyarakat. Negara-negara di Afrika hanya memiliki undang-undang sementara dan kebijakan dengan pendekatan *ad-hoc* dalam menangulangi *cybercrime.* Strategi dalam pemberantasan *cybercrime* dilakukan melalui kebijakan penal yakni dengan Kriminalisasi perbuatan dalam undang-undang sehingga terbuatan tersebut termasuk kejahatan di dunia maya, harmonisasi ketentuan hukum nasional dengan hukum internasional dalam memberantas *cybercrime* dan penegakan hukum melalui penjatuhan sanksi pidana bagi pelaku *cybercrime* serta kebijakan non penal yakni Menyusun kebijakan di luar hukum pidana yang mendukung upaya pencegahan

cybercrime, melakukan sosialisasi terhadap potensi kejahatan di dunia maya, membangun kerjasama dengan pihak swasta untuk membangun sistem keamanan di dunia maya dan membentuk jaringan kelembagaan dalam mencegah *cybercrime* baik dalam tataran nasional maupun dalam tingkat internasional.

Daftar Pustaka

Buku

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

Adami Chazawi, 2013, *Hukum Pidana Positif Penghinaan (Edisi Revisi),* Media Nusa Creative, Malang.

Ali Zaidan, 2015, *Menuju Pembaruan Hukum Pidana,* Sinar Grafika, Jakarta.

Andi Hamzah, 1987, *Aspek-aspek Pidana di Bidang Komputer,* Sinar Grafika, Jakarta.

Badan Pembinaan Hukum Nasional (BPHN), 2009, "Kajian *EU Convention on Cybercrime* dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi", Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, Jakarta.

Barda Nawawi Arief, 2005, *Pembaharuan Hukum Pidana; Dalam Perpekstif Kajian Perbandingan,* Citra Aditya Bakti, Bandung

Bederman, David J. 2008, *Globalization and International Law,* Palgrave Macmillan, New York.

Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi Regulasi & Konvergensi,* Refika Aditama, Bandung.

Dikdik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law: Aspek Hukum Teknologi Informasi,* Refika Aditama, Bandung.

Edmon Makarim, 2004, *Kompilasi Hukum Telematika,* PT RajaGrafindo Persada, Jakarta.

Gercke, Marco, 2012, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* ITU Telecommunication Development Bureau.

Hagan, Frank E., 1989, *Introduction Criminology Theories, Method and Criminal Behavior,* Nelson-Hall Inc., Chicago.

Hatta, 2010, *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan,* Pustaka Pelajar, Yogyakarta.

Mukhlis Taib, 2017, *Dinamika Perundang-undangan di Indonesia,* Refika Aditama, Bandung.

Muladi dan Diah Sulistyani R.S., 2016, *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal,* Alumni, Bandung.

Saleh, Roeslan, 1988, *Dari Lembar Kepustakaan Hukum Pidana*, Sinar Grafika, Jakarta.

Secretary of State for the Home Department, 2010, *Cyber Crime Strategy*, The Stationery Office Limited, London.

Smith, Scott S, 2016*, Internet Crime Report, Federal Bureau of Investigation,* Internet Crime Complaint Center, Washington D.C.

Soejadi, 2017, *Refleksi Mengenai Hukum dan Keadilan Akualisasinya di Indonesia,* Aswaja Presindo, Yogyakarta.

Soejadi, 2017, *Refleksi Mengenai hukum dan Keadilan;; Aktualisasinya di Indonesia,* Aswaja Pressindo, Yogyakarta.

Soekanto, Soerjono, 1981, *Kriminologi: Suatu Pengantar,* Cetakan Pertama, Ghalia Indonesia, Jakarta.

Sri Widoyati Wiratmo Soekito, 1983, *Anak dan Wanita dalam Hukum,* LP3ES, Jakarta.

Suteki, 2013, *Hukum dan Alih Teknologi; Sebuah Pergulatan Sosiologis,* Thafa Media, Yogyakarta.

Topo Santoso, 1997*, Seksualitas dan Hukum Pidana,* IND-HIL-CO, Jakarta.

UNODC, 2013*, Comprehensive Study on Cybercrime,* United Nations New York.

Jurnal

Barclay, Corlane "Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model

(CyberLeg-DPM)", *Information Technology for Development,* 2014 Vol. 20, No. 2, 165–195.

Etges, Rafael and Emma Sutcliffe, "An Overview of Transnational Organized Cyber Crime", *Information Security Journal: A Global Perspective*, 17:87–94, 2008.

Kasuri, Zubair; Karachi Flare, "Cybercrime Prevention Law Takes Effect", *Karachi* Vol. 12, Iss. 11, (Aug 2016).

Litska Strikwerda, "Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension", *Information & Communications Technology Law*, 2014 Vol. 23, No. 1.

Mayer, Jonathan, "Cybercrime Litigation", *University of Pennsylvania Law Review*, Vol. 164, 2016.

Olowu, Dejo, "Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa*", Journal of Information, Law & Technology,* 1, 2009.

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", *International Journal of Cyber Criminology* Vol 8 Issue 1 January - June 2014.

Watney, Murdoch "Cybercrime regulation at a cross-road: state and transnational laws versus global laws" *International Conference on Information Society* (i-Society 2012).

Artikel Elektronik

Elsam, "Mengenal Protokol Opsional Konvensi Hak Anak Mengenai Penjualan Anak, Prostitusi Anak dan Pornografi Anak", Elsam, http://lama.elsam.or.id/mobileweb/article.php?act=content&m=16&id=2819&cid=6024&lang=in, diakses pada 19 September 2018.

FBI, "Cyber Crime", https://www.fbi.gov/investigate/cyber, diakses pada 12 Desember 2017.

___, "FBI's Cybercrime Report 2017", https://www.cybersecurityintelligence.com/blog/fbis-cybercrime-report-2017-2575.html, diakses pada 12 Desember 2018.

Lona Olavia, "Cybercrime Threat a Growing Concern: Police", http://www.jakartaglobe.beritasatu.com/news/cyber crime-threat-growing-concern-police/, diakses pada 12 Desember 2018.

Ministry of Home Affairs, "National Cybercrime Action Plan", https://www.mha.gov.sg/Newsroom/press-releases/PublishingImages/Pages/Launch-of-the-, diakses pada 12 Desember 2017. National-Cybercrime-Action-Plan-at-RSA-Conference-Asia-Pacific-Japan/NCAP%20Document.pdf, diakses pada 12 Desember 2018.