Jurnal Lex Suprema
ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Artikel

UPAYA POLISI REPUBLIK INDONESIA DALAM MENANGGULANGI KEJAHATAN CYBERCRIME

THE POLICE OF THE REPUBLIC INDONESIA IN REDUCING CRIME CYBERCRIME

Ridho Iwan Saputra[1], Dany Ghufron[2], Riffa Kho[3]
Fakultas Hukum Universitas Balikpapan
Jl. Pupuk Raya, Gn. Bahagia, Kec. Balikapapan Selatan, Kota Balikpapan, Kalimantan Timur
Email: ridhoiwans@gmail.com

ABSTRAK
Dampak negatif dari perkembangan teknologi informasi dan komunikasi juga dirasakan oleh negara Indonesia, di mana kasus-kasus yang berkaitan dengan cybercrime banyak terjadi, salah satunya kasus carde. Pada Penelitian yang terdahulu khususnya motif *carder* di Indonesia dalam melakukan aksinya hampir sama dengan *cyber stalking*, yaitu mendapatkan atau membeli suatu barang tanpa harus membayar barang apa yang mereka beli tapi dengan menggunakan uang orang lain. Berdasarkan uraian tersebut, mendorong peneliti untuk melakukan penelitian dengan judul Upaya Polisi Republik Indonesia dalam menanggulangi kejahatan cybercrime, dengan rumusan masalah Bagaimanakah upaya Polri dalam menanggulangi cybercrime. Metode pendekatan yang digunakan dalam penelitian ini adalah penelitian hukum normatif. Adapun bentuk penanggulangan yang dilakukan oleh Polri, meliputi 2 jenis yaitu penanggulangan yang bersifat preventif dan penanggulangan yang bersifat refresif. Pasal 32 ayat (1) Undang- Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa . "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik".

Kata Kunci: *Cybercrime,* Polisi, Hukum.

ABSTRACT
The negative impact of the development of information and communication technology is also felt by the Indonesian state, where many cases relating to cybercrime occur, one of which is carde cases. In previous studies, especially carder motives in Indonesia in doing the action is almost the same as cyber stalking, which is getting or buying an item without having to pay for what they buy but using other people's money. Based on the description, encourage the authors to conduct research with the title The Indonesian Police's Efforts in tackling cybercrime crimes, with the formulation of the problem How is Polri's effort in tackling cybercrime. The method used in this research is normative legal research. The form of countermeasures carried out by the Police, includes 2 types, namely countermeasures that are preventive and countermeasures that are repressive. Article 32 paragraph (1) of Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions states that: "Every person intentionally and without rights or against the law in any way changes, adds, reduces, transmits, destroys, removes , transfer, hide any electronic information and / or electronic documents belonging to other people or public property ".

Keywords*: Cybercrime, Police, Law*

[1] Fakultas Hukum
[2] Fakultas Hukum
[3] Fakultas Hukum

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Artikel

I. PENDAHULUAN

A. Latar Belakang

Keresahan masyarakat terhadap cybercrime telah menjadi perhatian dunia internasional, terbukti dengan dijadikannya masalah *cybercrime* sebagai salah satu topik bahasan pada Kongres Perserikatan Bangsa- Bangsa (selanjutnya disebut PBB) ke-8 yang dilaksanakan di Havana, Cuba pada tahun 1990 dan Kongres PBB ke-10 yang diselenggarakan di Wina pada tahun 2000. Kongres PBB ke-8 di Havana, memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer *(computer related* crime), sedangkan pada Kongres PBB ke-10 di Wina, *cybercrime* dijadikan sebagai topik bahasan tersendiri dengan judul *crimes related to computer network*.

Dampak negatif dari perkembangan teknologi informasi dan komunikasi juga dirasakan oleh negara Indonesia, di mana kasus-kasus yang berkaitan dengan *cybercrime* banyak terjadi, salah satunya kasus *cybercrime*.

Pada Penelitian yang terdahulu khususnya motif carder di Indonesia dalam melakukan aksinya hampir sama dengan *cyber stalking*, yaitu mendapatkan atau membeli suatu barang tanpa harus membayar barang apa yang mereka beli tapi dengan menggunakan uang orang lain. Penjelasan dari Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa "UU ITE memiliki jaringan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atai dilakukan oleh warga negara Indonesia tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia, baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas teritorial atau universal". Penelitian sebelumnya dengan judul Peranan POLRI Dalam Menanggulangi *Cybercrime* (sudi kasus di POLRES Semarang)[4].

Dilihat dari perspektif hukum pidana, upaya penanggulangan *cyber crime* khususnya di Indonesia dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana); aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian); dan aspek jurisdiksi. Hal lain yang juga patut mendapat perhatian adalah tindakan penyidikan terhadap cyber crimedalam upaya mengungkap dan memberikan sanksi bagi setiap pelaku cyber crime.[5] Upaya Polri dalam pencegahan dan penanggulangan *cybercrime*, banyak menemui kendala, baik kendala yang berasal dari intern Polri maupun kendala yang berasal dari ekstern Polri.

Berdasarkan uraian di atas, mendorong penulis untuk melakukan penelitian dengan judul: "UPAYA POLISI REPUBLIK INDONESIA DALAM MENANGGULANGI *CYBERCRIME*". Perbedaan dari penelitian yang sebelumnya adalah terletak pada Peran yang dilakukan POLRI dalam menanggulangi *Cyber Crime.*

B. Rumusan Masalah

Dari uraian tersebut di atas maka penulis mengangkat permasalahan dalam penelitian ini, adalah Bagaimanakah upaya Polri dalam menanggulangi *cybercrime*?.

[4] Muhammad Friki Wicaksono, "PERANAN POLRI DALAM PENANGGULANGAN CYBER CRIME (Studi Kasus Di Polrestabes Semarang)" (PhD Thesis, Fakultas Hukum UNISSULA, 2017).

[5]Marwin Marwin, "Penanggulangan Cyber Crime Melalui Penal Policy," *ASAS* 5, no. 1 (2013)..

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

C. Metode Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah penelitian hukum normatif. Penelitian hukum normatif adalah penelitian hukum yang meletakkan hukum sebagai sistem norma. Sistem norma yang dimaksud adalah mengenai asas- asas, norma, kaidah dari peraturan perundang-undangan, putusan pengadilan, perjanjian serta doktrin (ajaran).

D. Tinjauan Pustaka

1. Tinjauan Umum Tentang Polisi

a. Pengertian Polisi

Polisi adalah suatu pranata umum sipil yang menjaga ketertiban, keamanan, dan penegakan hukum di seluruh wilayah Negara. Kepolisian adalah salah satu lembaga penting yang memainkan tugas utama sebagai penjaga keamanan, ketertiban dan penegakan hukum, sehingga lembaga Kepolisian ada di seluruh Negara berdaulat. Kepolisian merupakan alat negara yang bertugas untuk memelihara keamanan dan ketertiban masyarakat, diantaranya melawan kejahatan, akhirnya Kepolisian yang akan menentukan secara konkret apa yang disebut sebagai penegakan ketertiban. Pasal 1 angka 1 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia menjelaskan bahwa Kepolisian adalah segala ikhwal yang berkaitan dengan fungsi dan lembaga Polisi yang berkaitan peraturan perundang-undangan. Pasal 2 Kepolisian menyebutkan bahwa fungsi Kepolisian sebagai salah satu fungsi pemerintah Negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, pelindung, pengayom dan pelayan kepada masyarakat, sedangkan lembaga Kepolisian adalah organ pemerintah yang ditetapkan sebagai suatu lembaga dan diberikan kewenangan untuk menjalankan fungsinya berdasarkan peraturan perundang-undangan. Pasal 5 UU Kepolisian menyebutkan bahwa:

1) Kepolisian Negara Republik Indonesia merupakan alat yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakan hukum serta memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat dalam rangka terpeliharanya keamanan dalam negeri.
2) Kepolisian Negara Republik Indonesia adalah Kepolisian nasional yang merupakan satu kesatuan dalam melaksanakan peran sebagaimana dimaksud dalam ayat (1).

b. Tugas dan Fungsi Kepolisian

Tugas Kepolisian dapat diwujudkan apabila aparaturnya mampu melaksanakan tugasnya dengan baik, benar dan bertanggung jawab, dengan memberikan pelayanan pada masyarakat secara optimal. Tugas kepolisian merupakan bagian dari pada tugas negara dan untuk mencapai keseluruhan tugas itu, maka diadakanlah pembagian tugas agar mudah dalam pelaksanaan dan juga koordinasi, karena itulah di bentuk organisasi Polisi yang kemudian mempunyai tujuan untuk mengamankan dan memberikan perlindungan kepada masyarakat yang berkepentingan, terutama mereka yang melakukan suatu tindak pidana.

Tugas polisi adalah bagian daripada tugas negara perundang- undangan dan pelaksanaan untuk menjamin tata tertib ketentraman dan keamanan, menegakkan negara, menanamkan pegertian, ketaatan dan kepatuhan. Tugas kepolisian dalam Keputusan Presiden Republik Indonesia Nomor 7 Tahun 1974 dalam pasal 31 huruf a adalah sebagai berikut:[6] "Kepolisian

[6] WAHYU MEILANO, "PENERAPAN SANKSI PIDANA TERHADAP PELAKU TINDAK PIDANA POLITIK UANG PADA PEMILIHAN KEPALA DAERAH (STUDI KASUS PUTUSAN NOMOR: 238/PID. SUS/2018 PN. LHT)" (PhD Thesis, Universitas Muhammdiyah Palembang, 2019), hlm 136.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Negara Republik Indonesia disingkat Polri bertugas dan bertanggung jawab untuk melaksanakan segala usaha dan kegiatan sebagai alat negara dan penegak hukum terutama di bidang pembinaan keamanan dan ketertiban masyarakat, sesuai dengan Undang-Undang Nomor 13 Tahun 1961 dan Keputusan Presiden Nomor 52 Tahun 1969".

Adanya berbagai peraturan perundang-undangan yang mengatur tentang tugas Kepolisian seperti yang disebutkan di atas, maka jelaslah bahwa tugas Kepolisian sangat luas yang mencakup seluruh instansi, sampai pada masyarakat kecil, semua membutuhkan Polisi sebagai pengaman dan ketertiban masyarakat. Kepolisian dalam melaksanakan tugas serta membina keamanan dan ketertiban masyarakat, berkewajiban dengan segala usaha pekerjaan dan kegiatan untuk membina keamanan dan ketertiban masyarakat. Polisi sebagai pengayom masyarakat yang memberi perlindungan dan pelayanan kepada masyarakat bagi tegaknya ketentuan peraturan perundang- undangan, tidak terlepas dari suatu aturan yang mengikat untuk melakukan suatu tindakan dalam pelaksanaan tugasnya.

Kejahatan dalam perspektif kriminologi, bukan saja perbuatan yang melanggar undang-undang atau hukum pidana tetapi lebih luas lagi mencakup setiap perbuatan anti sosial yang merugikan masyarakat, meskipun perbuatan tersebut belum atau tidak diatur oleh undang-undang atau hukum pidana, hal tersebut menunjukkan bahwa peranan polisi dalam menegakkan hukum memiliki posisi yang sangat penting karena mereka berhubungan langsung dengan masyarakat maupun pelanggar hukum. Kepolisian merupakan salah satu lembaga dalam sistem peradilan pidana yang diberi wewenang untuk melakukan penyelidikan dan penyidikan terhadap peristiwa kejahatan, sebagaimana dijelaskan dalam Pasal 1 angka 13 UU Kepolisian.

Kepolisian merupakan aparat penegak hukum yang langsung berhadapan dengan masyarakat. Polisi diberi ruang oleh hukum untuk mengambil berbagai tindakan yang diperlukan menurut pertimbangan sesaat pada waktu kejadian berlangsung. Polisi diperbolehkan untuk melakukan penangkapan dan penahanan terhadap orang yang dicurigai telah melakukan kejahatan berdasarkan bukti-bukti dan aturan hukum yang telah ditetapkan. Polisi juga diberi kewenangan untuk meminta keterangan kepada setiap warga masyarakat yang mengetahui jalannya suatu kejahatan untuk dijadikan saksi yang diperlukan dalam proses pemeriksaan tersangka pelaku kejahatan.

Pelaksanaan tugas dari Kepolisian akan langsung dilihat dan dirasakan oleh masyarakat. Pada kontak langsung dengan masyarakat inilah citra Polisi akan sangat ditentukan. Citra Polisi yang buruk di masyarakat dikarenakan Polisi kurang mampu bersikap mandiri dalam mengusut kasus kejahatan yang akan membawa dampak pada proses pemeriksaan pelaku kejahatan pada tahap berikutnya. Pasal 13 UU Kepolisian menyatakan bahwa "Tugas pokok Kepolisian Negara Republik Indonesia adalah :

a. Memelihara keamanan dan ketertiban masyarakat;
b. Menegakkan hukum; dan
c. Memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat".

C. Wewenang Kepolisian

Kepolisian memiliki wewenang yang diatur dalam Pasal 15 ayat (1) UU Kepolisian, yaitu sebagai berikut:

a) Menerima laporan dan/atau pengaduan;
b) Membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum;
c) Mencegah dan menanggulangi tumbuhnya penyakit masyarakat;
d) Mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

e) Mengeluarkan peraturan Kepolisian dalam lingkup kewenangan administratif Kepolisian;
f) Melaksanakan pemeriksaan khusus sebagai bagian dari tindakan Kepolisian dalam rangka pencegahan;
g) Melakukan tindakan pertama di tempat kejadian;
h) Mengambil sidik jari dan identitas lainnya serta memotret seseorang;
i) Mencari keterangan dan barang bukti;
j) Menyelenggarakan pusat informasi kriminal nasional;
k) Mengeluarkan surat izin dan/atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat;
l) Memberikan bantuan pengamanan dalam sidang dan pelaksanaan putusan pengadilan, kegiatan instansi lain, serta kegiatan masyarakat;
m) Menerima dan menyimpan barang temuan untuk sementara waktu.

Wewenang Kepolisian untuk menyelenggarakan tugas di bidang proses pidana menurut Pasal 16 UU Kepolisian, adalah:

a) Melakukan penangkapan, penahanan, penggeledahan, dan penyitaan;
b) Melarang setiap orang meninggalkan atau memasuki tempat kejadian perkara untuk kepentingan penyidikan;
c) Membawa dan menghadapkan orang kepada penyidik dalam rangka penyidikan;
d) Menyuruh berhenti orang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri;
e) Melakukan pemeriksaan- pemeriksaan surat;
f) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
g) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
h) Mengadakan penghentian penyidikan;
i) Menyerahkan berkas perkara kepada penuntut umum
j) Mengajukan permintaan secara langsung kepada pejabat imigrasi yang berwenang di tempat pemeriksaan imigrasi dalam keadaan mendesak atau mendadak untuk mencegah atau menangkal orang yang disangka melakukan tindak pidana;
k) Memberi petunjuk dan bantuan penyidikan kepada penyidik pegawai negeri sipil untuk diserahkan kepada penuntut umum; dan
l) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

2. Tinjauan Umum Tentang Tindak Pidana

a. Pengertian Tindak Pidana

Istilah tindak pidana merupakan terjemahan dari istilah bahasa Belanda yaitu strafbaarfeit. Perkataan *"feit*" sendiri dalam bahasa Belanda berarti sebagian dari suatu kenyataan atau "*een gedeelte van de werkwlijkheid",* sedangkan *"strafbaar*" berarti dapat dihukum, sehingga secara harfiah perkataan strafbaarfeit dapat diterjemahkan sebagai sebagian dari suatu kenyataan yang dapat di hukum[7].

Pengertian tindak pidana tidak terdapat dalam KUHP, oleh karena itu dalam ilmu hukum terdapat beraneka ragam pengertian tindak pidana yang dikemukakan oleh para sarjana hukum. Tindak pidana adalah suatu perbuatan yang pelakunya dapat dipidana.[8]Tindak pidana adalah suatu kelakuan manusia yang diancam pidana oleh

[7]Mochamad Guruh Abdi Priatna and R. A. S. Hernawati, "Tindak Pidana Penodaan Agama Oleh Pemeluknya Melalui Media Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Kitab Undang-Undang Hukum Pidana," *Wacana Paramarta: Jurnal Ilmu Hukum* 16, no. 3 (2017): hlm 6.

[8] Wiryono Projodikoro, *Asas-Asas Hukum Pidana Di Indonesia* (Eresco, 1969), hlm 5.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

peraturan perundang- undangan, jadi suatu kelakuan yang pada umumnya dilarang dengan ancaman pidana[9].Tindak pidana adalah perbuatan manusia yang termasuk dalam ruang lingkup rumusan tindak pidana, bersifat melawan hukum dan dapat di cela[10].

1) Unsur-Unsur Tindak Pidana

Unsur tindak pidana menurut Simons, antara lain

a) Perbuatan tersebut diancam dengan pidana;
b) Perbuatan tersebut melawan hukum;
c) Perbuatan tersebut dilakukan dengan kesalahan; dan
d) Perbuatan tersebut dilakukan orang yang mampu bertanggung jawab.

Tindak pidana pada umumnya dapat dijabarkan ke dalam unsur-unsur yang pada dasarnya dapat dibagi menjadi 2 (dua) macam, antara lain [11]:

a) Unsur-unsur subjektif yaitu unsur-unsur yang melekat pada diri pelaku atau yang berhubungan dengan diri pelaku dan termasuk di dalamnya yaitu segala sesuatu yang terkandung di dalam batinnya. Unsur-unsur tersebut antara lain kesengajaan *(dollus*) atau ketidaksengajaan (*culpa*), memiliki maksud (*vornemen*) pada suatu percobaan (*poging*), maksud (*oogmerk*), merencanakan terlebih dahulu *(voorhedachteraad*) serta perasaan takut atau stress.
b) Unsur-unsur objektif yaitu unsur-unsur yang ada hubungannya dengan keadaan-keadaan mana tindakan-tindakan dan pelaku itu harus melakukan. Unsur-unsur yang termasuk di dalamnya antara lain sifat melanggar hukum, kualitas dari pelaku, kausalitas yaitu hubungan antara sesuatu tindakan sebagai penyebab dengan sesuatu kenyataan sebagai akibatnya.

2) Subjek Tindak Pidana

Sistem KUHP menyatakan, yang dapat menjadi subjek tindak pidana adalah manusia, hal ini dapat dilihat dalam perumusan-perumusan dari tindak pidana dalam KUHP, yang menampakkan daya berpikir sebagai isyarat bagi subjek tindak pidana itu, juga terlibat pada wujud hukuman atau pidana yang termuat dalam Pasal 10 Kitab Undang-Undang Hukum Pidana (KUHP) yaitu hukuman penjara, kurungan dan denda.

Hal-hal yang menyatakan bahwa manusia sebagai subjek tindak pidana adalah:

a) Terdapatnya perumusan tindak pidana yang dimulai dengan perkataan barang siapa, seorang ibu, seorang pejabat, seorang nahkoda.
b) Jenis-jenis pidana yang ditentukan dalam Pasal 10 KUHP hanya ditujukan terhadap manusia
c) Dalam hukum pidana yang berlaku sekarang menganut asas kesalahan seseorang manusia yang disebut dengan "hukum pidana kesalahan". Dalam Schuldstrafrecht yang dianggap dapat berbuat kesalahan hanyalah manusia yaitu yang berupa "kesalahan perorangan atau individual".[12]

Hukum pidana pada perkembangannya mengenai subjek tindak pidana itu diperluas, bukan saja hanya manusia, tetapi juga badan hukum ataupun koorporasi terutama dalam hal perpajakan, perekonomian, dan keamanan negara yang diatur dalam peraturan perundang-undangan di luar KUHP. Pasal 59 dan Pasal 169 KUHP menentukan bahwa badan hukum sebagai subjek hukum yang dapat dikenai pidana, namun ternyata yang dapat dikenakan pidana hanya manusia yang ikut perkumpulan bukan badan hukumnya.

[9] *Bambang Poernomo, 1983, Asas-Asas Hukum Pidana, Jakarta, Ghalia Indonesia, Hlm. 91*, n.d.
[10]Muhamad Iqbal, S. Suhendar, and Ali Imron, "Hukum Pidana," 2019, hlm 88.
[11] P. A. F. Lamintang, "Dasar-Dasar Hukum Pidana Indonesia, Bandung: PT," *Citra Aditya Bakti*, 1997, hlm. 183.
[12]*Tongat, 2003, Hukum Pidana Materiil, Jakarta, Djambatan, Hlm. 24*, n.d..

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Berdasarkan ketentuan yang ada di dalam KUHP badan hukum tidak dapat dipidana, yang dapat dikenakan pidana hanyalah pengurus dari badan hukum tersebut saja.

b. Penggolongan Tindak Pidana

Hukum pidana mengenal juga istilah jenis-jenis tindak pidana. Atang Ranoemihardja mengatakan jenis-jenis tindak pidana tersebut adalah kejahatan tindak pidana yang tercantum dalam buku II Pasal 104 KUHP sampai dengan Pasal 448 KUHP, pelanggaran tindak pidana yang tercantum dalam buku III Pasal 449 KUHP sampai dengan Pasal 569 KUHP, jenis-jenis tindak pidana adalah:

a) Tindak pidana formal, yaitu tindak pidana yang selesai setelah perbuatan itu dilakukan dan terhadap perbuatan tersebut diancam dengan hukuman, walaupun ada tidaknya "akibat" dari perbuatan.
b) Tindak pidana materil, yaitu tindak pidana yang selesai setelah timbul dari akibat perbuatan
c) Tindak pidana komisionis, yaitu melakukan pelanggaran atau berbuat sesuatu yang dilarang oleh undang-undang.
d) Tindak pidana ommisionis, yaitu tidak melakukan atau tidak berbuat sesuatu yang diperintahkan oleh undang- undang.
e) Tindak pidana yang tersendiri, terdiri dari:[13]
   1) *Concursus idealis*
      Tindak pidana yang terjadi karena dengan dilakukannya hanya satu perbuatan materi saja, maka sebenarnya perbuatan itu melanggar beberapa ketentuan pidana sekaligus, seperti diatur dalam Pasal 63 KUHP.
   2) *Concursus realis*
      Tindak pidana ini terjadi dalam hal beberapa fakta yang harus dipandang sebagai suatu perbuatan yang terdiri dan masing- masing diantara peristiwa pidana, dilakukan oleh satu orang dan diantara waktu terjadinya masing-masing fakta itu tidak ada putusan hukuman terhadap salah satu fakta tersebut.
f) Perbuatan terus menerus, yaitu beberapa perbuatan yang berhubungan sedemikian rupa sehingga harus dipandang sebagai suatu perbuatan yaitu diteruskan, mengenai perbuatan terus menerus ini diatur dalam Pasal 64 KUHP.
g) Tindak pidana yang selesai seketika, yaitu tindak pidana yang terdiri dari satu atau beberapa perbuatan tertentu yang menimbulkan suatu akibat tertentu yang selesai dalam jangka waktu yang singkat
h) Tindak pidana yang meneruskan keadaan terlarang, yaitu perbuatan yang juga meneruskan keadaan terlarang yang telah ada.
i) Tindak pidana majemuk, yaitu pembuat dihukum setelah tindak pidana ini dilakukan secara berturut-turut.
j) Tindak pidana tunggal, yaitu satu tindak pidana saja, tindak pidana itu dilakukan maka sudah cukup untuk menetapkan hukuman terhadap pembuatnya.
k) Tindak pidana yang kualifikasi, yaitu suatu bentuk istimewa dari tindak pidana dasar dan mengandung semua unsur tindak pidana dasar ditambah satu atau beberapa anasir lainnya yang menjadi alasan untuk memperberat hukuman terhadap pembuat.
l) Tindak pidana sengaja, yaitu tindak pidana yang dikehendaki dan diketahui.
m) Tindak pidana kealpaan, ada beberapa istilah yang dipakai untuk menyatakan kealpaan yaitu kekhilapan, kelalaian, patut dapat menduga dan tidak berhati-hati.

[13] Ibid, hlm. 29

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

n) Tindak pidana jabatan, yaitu tindak pidana yang hanya dapat dilakukan oleh orang yang mempunyai jabatan seperti pegawai negeri, anggota TNI, dan lain sebagainya.
o) Tindak pidana aduan, yaitu suatu tindak pidana yang hanya dapat dituntut apabila yang dirugikan mengajukan pengaduan.

Jenis-jenis tindak pidana dalam Kitab Undang-Undang Hukum Pidana terbagi atas dua jenis, yaitu kejahatan (misdrijven) dan pelanggaran (*overtredingen*). Kedua jenis tindak pidana tersebut didasarkan kepada perbedaan asasi, Sofjan Sastrawidjaja mengatakan bahwa[14]: "Kejahatan adalah delik hukum, sedangkan pelanggaran adalah kejahatan undang-undang. Suatu perbuatan merupakan delik hukum, apabila sejak semula sudah dapat diketahui bahwa perbuatan tersebut telah bertentangan dengan hukum, sebelum ditentukan dalam undang- undang. Sedangkan delik undang-undang baru dapat dirasakan sebagai perbuatan yang bertentangan dengan hukum setelah ditentukan dalam undang-undang".

Akibat hukum dari kedua jenis tindak pidana itu menurut undang-undang memang berbeda, yaitu :[15]

a) Pidana penjara hanya diancamkan pada kejahatan, sedangkan pada pelanggaran tidak.
b) Pada kejahatan maka bentuk bersalah yaitu kesengajaan atau kealpaan pada pelaku tindak pidana harus dibuktikan, sedangkan pada pelanggaran hal ini tidak perlu dibuktikan.
c) Percobaan melakukan kejahatan dapat dipidana, sedangkan percobaan melakukan pelanggaran tidak dapat dipidana.
d) Pembantuan melakukan kejahatan dapat dipidana, sedangkan pembantuan melakukan pelanggaran tidak dapat dipidana. (Pasal 56 juncto Pasal 60 KUHP)
e) Gugurnya karena daluwarsa hak penuntutan pidana dan hak menjalankan pidana bagi kejahatan jangka waktunya lebih lama daripada pelanggaran (Pasal 78 juncto Pasal 84 KUHP)
f) Pasal 59 KUHP yang mengandung ancaman pidana terhadap pengurus dan komisaris suatu badan hukum, korporasi, dan yayasan, karena disangka telah melakukan suatu tindak pidana, hanya berlaku dalam hal pelanggaran.
g) Pengaduan sebagai syarat penuntutan dalam delik aduan hanya ditentukan untuk tindak pidana kejahatan.
h) Dalam hal perbarengan, sistem pemidanaan berbeda bagi kejahatan dan bagi pelanggaran. Dalam perbarengan jamak, dalam kejahatan berlaku stelsel serapan diperberat (Pasal 65 KUHP) dan stelsel kumulasi terbatas (Pasal 66 KUHP), sedangkan dalam pelanggaran berlaku stelsel kumulasi tidak terbatas (Pasal 70 KUHP)
i) Penyelesaian diluar sidang atau penebusan penuntutan pidana hanya mungkin dalam pelanggaran yang diancam dengan pidana denda (Pasal 82 KUHP)
j) Pelanggaran kejahatan karena kealpaan, maka perampasan barang tertentu sebagai pidana tambahan, hanya dapat dijatuhkan, jika hal ini disebutkan dengan tegas dalam undang-undang pidana (Pasal 39 ayat (2) KUHP), sedangkan dalam hal yang disengaja, perampasan barang-barang tertentu tersebut dapat juga dijatuhkan walaupun undang-undang pidana tidak menyebutkan dengan tegas hal itu.
k) Hak untuk menuntut pidana terhadap warga Negara Indonesia yang berada di luar wilayah Indonesia melakukan suatu tindak pidana tertentu, hanya berlaku dalam hal

[14] Ibid, hlm. 34
[15] Ibid, hlm. 38.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

dilakukan suatu kejahatan tertentu (Pasal 5 KUHP) tidak berlaku dalam hal dilakukan suatu pelanggaran.

l) Perundang-undangan hukum pidana Indonesia berlaku bagi setiap pejabat atau pegawai negeri yang diluar wilayah Indonesia yang melakukan salah satu kejahatan dalam Bab XXVIII Buku II KUHP (Pasal 7 KUHP), hal ini tidak dikenal dalam pelanggaran.

m) Hanya penadahan barang- barang yang diperoleh dari kejahatan yang dapat dipidana (Pasal 480 KUHP), sedangkan penadahan barang-barang yang diperoleh dari pelanggaran tidak dikenal.

n) Peraturan-peraturan khusus mengenai penyertaan yang ditentukan dalam Pasal 61 dan Pasal 62 KUHP kejahatan cetak, hanya berlaku dalam hal kejahatan.

3. Tinjauan Umum Tentang Cybercrime

a. Pengertian Cybercrime

Kejahatan dunia maya *(cybercrime)* muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Kepolisian Inggris mengemukakan bahwa *cybercrime* adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[16]. *Cybercrime* menurut Peter adalah*"The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the from of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money or sensitive information using a computer system".*[17]

Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[18]

Dokumen Kongres PBB yang dikutif oleh Barda Nawawi Arief, mengenai *The Prevention of Crime* and the *Treatment of Offenders di Havana* Cuba tahun 1990 dan di Wina Austria tahun 2000, menjelaskan adanya 2 (dua) istilah yang terkait dengan pengertian *cybercrime*, yaitu *cybercrime* dan *computer related crime*[19]. Back Ground Paper untuk lokakarya Kongres PBB tahun 2000 di Wina, istilah cybercrime lengkapnya, sebagai berikut :[20]

a) Cybercrime in a narrow sense (computer crime) : any legal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them; and

b) *Cyber crime in a broader sense (computer related crime) : any illegal behavior commited by means on in relation to, a computer system or network, including such*

[16] *Abdul Wahid Dan Mohammad Labib, 2005, Kejahatan Mayantara (Cybercrime), Jakarta, PT. Refika Aditama, Hlm. 40.*, n.d.

[17] *Peter Stephenson, 2000, Investigating Computer Telated Crime : A Handbook for Corporate Investigator, London, CRC Press, Hlm. 56.*, n.d.

[18] "Indra Safitri, 'Tindak Pidana Di Dunia Cyber', (Http://Business.Fortunecity.Com/Buffett/842/ Art180199_tindakpidana.Html), Diakses 15 Januari 2015.," n.d.

[19] S. H. Barda Nawawi Arief, *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan* (Prenada Media, 2018), hlm 24.

[20] Ibid, hlm. 26.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

crime as illegal possession, offering or distributing information by means of a computer system or network.

b. Jenis-Jenis Cybercrime

Kejahatan yang berhubungan erat dengan penggunaan teknologi berbasis komputer dan jaringan telekomunikasi dikelompokkan dalam beberapa bentuk sesuai modus operandi, yaitu :[21]

a) Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku melakukannya dengan maksud sabotase atau pencurian informasi penting dan rahasia. Kejahatan ini semakin berkembang seiring dengan berkembangnya teknologi internet.

b) Illegal Contents

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

c) Data Forgery

Merupakan kejahatan dengan memasukkan data pada dokumen - dokumen penting yang tersimpan sebagai *scripless document* melalui internet.

d) Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran.

e) Cyber Sabotage and Extortion

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

f) Offense Aggainst Intellectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet.

g) Infringements of Privacy

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immaterial.

II.PEMBAHASAN

Produk inovasi teknologi telekomunikasi, salah satunya adalah internet *(interconnection networking)*, yaitu suatu koneksi antar jaringan komputer. Internet saat ini telah memasuki berbagai segmen aktivitas manusia, baik dalam sektor politik, sosial, budaya, ekonomi dan bisnis maupun dalam sektor pemerintahan. Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(borderless).*

[21] "Suara Merdeka, 'Situs Internet' (Http://Www.Suaramerdeka.Com/Harian/0207/24/Nas13. Html), Diakses 12 Januari 2015."

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Kehidupan manusia modern saat ini tidak dapat dilepaskan dari bahkan terkadang sangat bergantung pada kemajuan teknologi canggih/maju (*high tech atau advanced technology*) di bidang informasi dan elektronik melalui jaringan internasional (internet). Media internet pada instansi pemerintahan mulai banyak dimanfaatkan dengan membuat suatu situs internet instansi pemerintahan tersebut, yang dimaksudkan agar masyarakat dapat dengan mudah mencari informasi yang berhubungan dengan instansi yang dimaksud hanya dengan mengakses situs instansi pemerintahan tersebut melalui media internet.

Cybercrime, berdasarkan pada uraian di atas merupakan sebuah isu hukum internasional. Perbedaannya, di beberapa negara anggota PBB sudah meratifikasi hasil kongres internasional mengenai *cybercrime* dalam sebuah regulasi peraturan perundang- undangan secara khusus, sedangkan di yaitu penanggulangan yang bersifat preventif dan penanggulangan yang bersifat refresif.

Penanggulangan yang bersifat preventif, dilakukan Polri, melalui berbagai kegiatan, antara lain :[22]

a) Upaya-upaya pencegahan;
b) Upaya-upaya penanggulangan;
c) Upaya edukatif, dan yang terakhir apabila tidak teredukasi: maka:
d) Upaya-upaya penegakan hukum

Penanggulangan yang bersifat refresif adalah langkah-langkah yang dilakukan Polri apabila kejahatan cybercrime sudah terlanjur terjadi. Penegakan hukum yang dilakukan oleh Polri terhadap pelaku kejahatan *cybercrime*, didasarkan pada ketentuan Pasal 32 ayat (1) UU ITE, yang berbunyi: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik".

Pasal 32 ayat (1) UU ITE mengandung unsur-unsur tindak pidana, baik unsur subjektif maupun unsur objektif. Unsur subjektif dari tindak pidana sebagaimana yang tercantum dalam Pasal 32 ayat (1) UU ITE adalah unsur dengan sengaja dan unsur melawan hukum, sedangkan unsur objektifnya adalah unsur mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan dan unsur suatu sistem Indonesia sendiri pengaturan mengenai *cybercrime*. Adapun bentuk penanggulangan yang dilakukan oleh Polri, meliputi 2 jenis elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.

Pasal 1 angka 1 UU ITE menyebutkan bahwa "Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic* data interchange (selanjutnya disebut EDI), 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". Pasal 1 angka 4 UU ITE, kemudian menyebutkan"Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya".Pasal 1 angka 5 UU ITE kemudian menyebutkan pula "Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis,

[22] "Kepala Biro Multimedia Mabes Polri Brigadir Jenderal Yan Fitri Halimansyah (Suara.Com/Maidian Reviani), Jum'at, 08 September 2017.," n.d.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik".

Penyidik Polri dalam kaitannya dengan kejahatan *carding* sulit untuk membuktikannya karena semua alat bukti yang ada berbentuk informasi dan atau dokumen elektronik, namun cetaknya merupakan alat bukti hukum yang sah". Pasal 5 ayat (2), juga menyebutkan bahwa: "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia".

Dengan demikian, alat bukti yang dapat digunakan penyidik Polri terkait dengan kejahatan *cybercrime* dapat diperluas dari ketentuan alat bukti sebagaimana yang telah diatur dalam Pasal 184 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (selanjutnya disebut KUHAP), yaitu bahwa alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa.

Ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah diatur dalam pasal tersebut tidak dapat ditambah atau dikurangi[23].

Secara umum terdapat beberapa teori mengenai sistem pembuktian, yaitu:

1. *Convention in time theory*, yaitu sistem pembuktian yang menyatakan bahwa salah tidaknya seorang terdakwa semata-mata ditentukan oleh penilaian keyakinan hakim. Keyakinan hakim ini dapat diperoleh melalui alat-alat bukti yang diajukan dalam persidangan;
2. *Convention reisonee theory*, yaitu sistem pembuktian berdasarkan keyakinan hakim untuk menentukan salah tidaknya hak ini dapat dijadikan sebagai alat bukti sebagaimana ditentukan dalam Pasal 5 ayat (1) UU ITE, yang berbunyi : "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil terdakwa, namun dalam sistem ini keyakinan hakim dibatasi dan harus didasari dengan alasan-alasan yang jelas dan dapat diterima yang wajib diuraikan dalam putusannya;
3. Teori pembuktian menurut undang- undang secara positif, yaitu pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *convention in time theory.* Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah ditetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa; dan
4. Teori pembuktian menurut undang- undang secara negatif, yaitu sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *convention in time theory.* Rumusan teori ini adalah bahwa salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pad acara dan dengan alat- alat bukti yang sah menurut undang- undang[24].

Sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *convention in time theory*, hal ini terlihat dari ketentuan Pasal 183 KUHAP yang menegaskan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah, hakim memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya.

[23]Munir Fuady, "Teori Hukum Pembuktian (Pidana Dan Perdata)," *Bandung: Citra Aditya*, 2006, hlm 23..

[24] M. Yahya Harahap, "Pembahasan Permasalahan Dan Penerapan KUHAP Edisi Kedua," *Sinar Grafika, Jakarta*, 2002, hlm 291.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Berbicara mengenai alat bukti petunjuk, tidak terlepas dari ketentuan Pasal 188 ayat (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk yang secara limitatif hanya dapat diperoleh dari keterangan saksi, surat, keterangan terdakwa[25]. Berdasarkan hal ini, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti tersebut. Umumnya, alat bukti petunjuk baru diperlukan apabila alat bukti lainnya belum mencukupi batas minimum pembuktian yang diatur dalam Pasal 183 KUHAP, sehingga alat bukti petunjuk merupakan alat bukti yang bergantung pada alat bukti lainnya yaitu alat bukti saksi, surat, dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian[26].

Petunjuk sebagai alat bukti, juga tidak dapat berdiri sendiri membuktikan kesalahan terdakwa karena hakim tetap terikat pada batas minimum pembuktian sesuai dengan ketentuan Pasal 183 KUHAP.

Polri dalam melakukan penegakan hukum terhadap kasus *cybercrime*, antara lain:

1) Personel Polri

Polri mengalami kesulitas dalam menghadapi kasus-kasus *cybercrime*, khususnya berkenaan dengan kejahatan carding, hal ini dilaterbelakangi oleh masih sedikitnya personel Polri yang memahami seluk beluk teknologi informasi (internet), di samping itu aparat personel Polri pun belum siap dalam mengantisipasi maraknya kejahatan cybercrime karena masih banyak personel Polri yang gagap teknologi, hal ini disebabkan oleh masih kurangnya dukungan teknologi yang berkaitan dengan jaringan internet.

2) Sarana dan Prasaran

Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut, salah satunya computer forensik untuk mengungkap data- data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (*image*, program dan lain sebagainya). Kenyataannya, computer forensic yang dimiliki oleh Polri dalam menangani *cybercrime*, masih belum memadai. Computer forensic diperlukan Polri, terutama untuk membuktikan jejak-jejak pelaku kejahatan *cybercrime* dalam melakukan aksinya terutama yang berhubungan dengan program dan data-data komputer.

3) Peraturan Perundang-Undangan

Indonesia telah mengesahkan UU ITE, namun undang-undang ini tidak mengatur secara khusus hal-hal yang menyangkut *cybercrime*. Ketentuan umum undang-undang ini tidak menggambarkan secara jelas tentang kejahatan-kejahatan dengan menggunakan. Ketentuan umum undang-undang ini tidak menggambarkan secara jelas tentang kejahatan-kejahatan dengan menggunakan computer.

Banyak ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam UU ITE, seperti kelalaian atau khilaf, padahal kelalaian dalam dunia maya adalah tindakan fatal yang dapat menimbulkan kerugian yang tidak sedikit, bahkan dapat menghancurkan sebuah negara. Kegiatan lain yang sama pentingnya dengan kelalaian adalah percobaan melakukan perbuatan jahat dan turut serta melakukan kejahatan (*deelneming*), di mana dalam UU ITE tidak diatur, apakah percobaan melakukan dan turut serta melakukan kejahatan dapat dipidana atau tidak. UU ITE juga tidak mengaur kapan kadaluwarsa perbuatan pidana.

[25] Ibid, hlm. 294.
[26] Ibid, hlm. 296.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Ancaman pidana yang dapat dijatuhkan bagi para pelaku kejahatan *cybercrime*, sebagaimana diatur dalam Pasal 32 ayat (1) UU ITE hanya dikenakan pidana penjara paling lama 8 (delapan) tahun serta pidana denda sebesar Rp.2.000.000.000,- (dua miliar rupiah). Ancaman sanksi bagi pelanggaran Pasal 32 ayat (1) UU ITE, tidak menggunakan ketentuan ancaman pidana minimal, sehingga tidak menutup kemungkinan hakim akan menjatuhkan putusan sanksi pidana yang sangat ringan, hal ini akan berakibat bahwa prevelensi umum dan khusus atas pemidanaan pelaku kejahatan *cybercrime* tidak tercapai. Dari Pembahasan yang sudah diuraikan baik oleh kedua peneliti yang sebelumnya maka dapat dipastikan bahwa yang dilakukan oleh POLRI sudah cukup maksimal dan peneliti setuju.

Cybercrime adalah salah satu produk dari globalisasi kejahatan, dimana kejahatan dilakukan tanpa terbatas pada ruang dan waktu. Muladi dan Diah Sulistyani R.S.[27] 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* yang bersifat bermusuhan *(adversarialism*) sebagai pendekatan represif dan dikombinasikan dengan pendekatan preventif mutualisme atau kebersamaan atas dasar *peacemaking criminology*[28].

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.[29] 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:

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[30]. 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[31]. Kriminalisasi perlu dilakukan dengan mempertimbangkan kepentingan hukum yang dilindungi supaya tidak terjadi *over*

[27] Diah Sulistyani Muladi, "Kompleksitas Perkembangan Tindak Pidana Dan Kebijakan Kriminal," *Bandung: Alumni*, 2016, hal 24.
[28] Ibid., hal. 24.
[29] Mohammad Hatta, *Kebijakan Politik Kriminal: Penegakan Hukum Dalam Rangka Penanggulangan Kejahatan* (Pustaka Pelajar, 2010), hal 39.
[30] Sri Widoyati Wiratmo Soekito, *Anak Dan Wanita Dalam Hukum* (Lembaga Penelitian, Pendidikan dan Penerangan Ekonomi dan Sosial, 1983), hal 85.
[31] Andi Hamzah, *Aspek-Aspek Hukum Pidana Dibidang Komputer* (Jakarta: Sinar Grafika, 1987), hal 28.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

kriminalisasi. Kriminalisasi memang memungkinkan kekacauan dalam struktur hukum telematika. Secara tegas Jonathan Mayer mengatakan sebagai berikut[32]:

> *"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[33] 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 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. Harmonisasi ketentuan hukum nasional dengan hukum internasional dalam memberantas cybercrime. Sigid Suseno [34] 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[35]) 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.

---

[32] Jonathan Mayer, "Cybercrime Litigation," *U. Pa. L. Rev.* 164 (2015): hal. 1485-1486..

[33] *Zubair Kasuri, Karachi Flare, "Cybercrime Prevention Law Takes Effect", Karachi Vol. 12, Iss. 11, (Aug 2016), Hal. 28,* n.d..

[34] *Sigid Susone, Op.Cit., Hal. 198,* n.d.

[35] "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.," n.d.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

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[36]. Penegakan hukum tersebut dilakukan untuk mewujudkan perubahan yang efektif di dalam masyarakat. 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[37].

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[38]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 element 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 c*ybercrim*e melalui sarana penal perlu diimbangi denggan kebijakan non penal. Kebijakan non penal yang dapat dilakukan adalah sebagai berikut:

[36] Dewi Bunga, "POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME," *Jurnal Legislasi Indonesia* 16, no. 1 (2019): hal 19.
[37] *Soejadi, 2017, Refleksi Mengenai Hukum Dan Keadilan;; Aktualisasinya Di Indonesia, Aswaja Pressindo, Yogyakarta, Hal. 56-57.*, n.d.
[38] Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2015).hal 100

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

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 *responsiv*e dan menyiapkan kelembagaan yang dapat melakukan tindakan cepat ketika terjadi masalah di dunia maya.

a) Pertanggungjawaban Pidana atau Pemidanaan

Pertanggungjawaban pidana pada hakikatnya mengandung pencelaan pembuat (subjek hukum) atas tindak pidana yang telah dilakukannya.Oleh karena itu, pertanggungjawaban pidana mengandung di dalamnya pencelaan/pertanggungjawaban objektif dan subjektif. Artinya, secara objektif si pembuat telah melakukan tindak pidana menurut hukum yang berlaku (asas legalitas), dan secara subjektif si pembuat patut dicela atau dipersalahkan/dipertanggungjawabkan atas tindak pidana yang dilakukannya itu (asas culpabilitas/kesalahan) sehingga ia patut dipidana.

Persyaratan dan asas-asas pertanggungjawaban pidana tersebut merupakan hal-hal yang sudah diterima secara umum dan konvensional dalam doktrin/teori, maupun dalam peraturan perundang-undangan (hukum positif). Untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhi persyaratan objektif, yaitu perbuatannya harus telah merupakan tindak pidana menurut hukum yang berlaku (asas legalitas).

Berdasarkan persyaratan objektif yang konvensional, pertanggungjawaban cyber crime tentunya harus didasarkan pada sumber hukum perundang-undangan yang berlaku saat ini, baik didalam KUHP maupun dalam undang-undang khusus di luar KUHP. Namun kenyataannya dalam peraturan perundang-undangan yang ada dan berlaku sekarang di Indonesia, tidak semua kasus cyber crime dapat dijangkau. Selain itu dalam peraturan perundang-undangan yang ada sekarang (baik KUHP maupun UU khusus di luar KUHP) memiliki berbagai kelemahan dan kemampuan sangat terbatas dalam menghadapi berbagai masalah cyber crime. Berbagai masalah atau kelemahan tersebut antara lain[39]:

1. Di dalam UU No.32 Tahun 2002 tentang penyiaran, tidak ada penentuan kualifikasi delik (sebagai kejahatan atau pelanggaran) sehingga dapat menimbulkan masalah yuridis;
2. Dalam berbagai undang-undang, terdapat subjek hukum berupa korporasi namun tidak membuat aturan tentang pertanggungjawaban pidana untuk korporasi, misalnya dalam UU No.36 Tahun 1999 tentang Telekomunikasi;

[39] Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Rajawali Press, PT RajaGrafindo Persada, Jakarta, 2006, hlm. 102-105

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

3. Dalam undang-undang yang mengatur pertanggungjawaban pidana korporasi (seperti dalam undang-undang korupsi dan pencucian uang), tidak diatur ketentuan mengenai aturan pidana pengganti denda untuk korporasi apabila denda tidak dibayar;
4. Dalam undang-undang yang memuat ancaman pidana minimal khusus, tidak ada ketentuan mengenai aturan atau pedoman penerapan pidana minimal khusus;
5. Pengakuan yuridis terhadap electronic record sebagai alat bukti hanya ada pada Undang undang Korupsi (UU No. 31 Tahun 1999 jo. UU No. 20 Tahun 2001, UU No. 30 Tahun 2002 tentang Pemberantasan Tindak Pidana Korupsi); dan Undang-Undang Tindak Pidana Pencucian Uang (UU No. 15 Tahun 2002), sehingga menjadi masalah apabila akan diterapkan untuk tindak pidana lainnya khususnya yang berkaitan dengan *cybercrime*.

Masih terbatasnya undang-undang yang ada khususnya yang mengatur *cybercrime,* berarti asas legalitas konvensional saat ini menghadapi tantangan serius dari perkembangan *cybercrime.* Hal ini dapat dimaklumi karena[40]

a. *Cybercrime* berada di lingkungan elektronik dan dunia maya yang sulit diidentifikasi secara pasti, sedangkan asas legalitas konvensional bertolak dari perbuatan riel dan kepastian hukum;.
b. *Cybercrime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah, sedangkan asas legalitas konvensional bertolak dari sumber hukum formal (undangundang) yang statis;
c. *Cybercrime* melampaui batas-batas negara, sedangkan perundang-undangan suatu negara pada dasarnya atau pada umumnya hanya berlaku di wilayah teritorialnya sendiri.

Pertanggungjawaban pidana pelaku *cybercrime* juga harus mengandung makna pencelaan subjektif. Artinya secara subjektif si pelaku patut dicela atau dipersalahkan atau dipertanggungjawabkan atas tindak pidana yang dilakukannya sehingga ia patut dipidana. Secara singkat sering dinyatakan, tiada pidana (pertanggungjawaban pidana) tanpa kesalahan (asas culpabilitas). Asas culpabilitas ini pun tentunya harus diperhatikan dalam masalah pertanggungjawaban pidana *cybercrime*. Walaupun mungkin menghadapi tantangan sendiri dalam kasus-kasus *cybercrime* karena tidak mudah membuktikan adanya unsur kesalahan *(dolus/culpa)* dalam masalah *cybercrime.*

III. PENUTUP

A. Kesimpulan

Berdasarkan pembahasan sebelumnya, maka dapat ditarik beberapa kesimpulan antara lain :Upaya Polri dalam menanggulangi *cybercrime* di Indonesia, dilakukan melalui upaya pereventif dan upaya refresif. Upaya preventif dilakukan dengan melakukan upaya pencegahan, upaya penanggulangan, upaya edukatif, dan yang terakhir apabila tidak teredukasi maka melaksanakan upaya penegakan hukum. Polri di bidang teknologi computer. Upaya represif, dilakukan dengan melakukan penegakkan hukum terhadap pelaku *cybercrime* didasarkan pada ketentuan hukum yang berlaku, yaitu Pasal 32 ayat (1) Undang- Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE).

B. Saran

Hal-hal yang ingin peneliti sampaikan dalam kesempatan ini, antara lain :
Pemerintah perlu melakukan revisi terhadap UU ITE atau membuat peraturan lain yang berhubungan dengan kejahatan cybercrime dan upaya pencegahan dan penanggulangan *cybercrime,* Polri hendaknya meningkatkan kerjasama bidang teknologi informasi dan

[40] *Barda Nawawi Arief, Tindak Pidana Hlm. 78.*, n.d.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

komunikasi dengan *NCB Interpol* serta masyarakat dalam menanggulangi kejahatan *cybercrime.*

DAFTAR PUSTAKA

Abdul Wahid Dan Mohammad Labib, 2005, Kejahatan Mayantara (Cybercrime), Jakarta, PT. Refika Aditama, Hlm. 40., n.d.

"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.," n.d.

Bambang Poernomo, 1983, Asas-Asas Hukum Pidana, Jakarta, Ghalia Indonesia, Hlm. 91, n.d.

Barda Nawawi Arief, S. H. Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan. Prenada Media, 2018.

Barda Nawawi Arief, Tindak Pidana Hlm. 78., n.d.

Bunga, Dewi. "POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME." Jurnal Legislasi Indonesia 16, no. 1 (2019): 1–15.

Fuady, Munir. "Teori Hukum Pembuktian (Pidana Dan Perdata)." Bandung: Citra Aditya, 2006.

Gillespie, Alisdair A. Cybercrime: Key Issues and Debates. Routledge, 2015.

Hamzah, Andi. Aspek-Aspek Hukum Pidana Dibidang Komputer. Jakarta: Sinar Grafika, 1987.

Harahap, M. Yahya. "Pembahasan Permasalahan Dan Penerapan KUHAP Edisi Kedua." Sinar Grafika, Jakarta, 2002.

Hatta, Mohammad. Kebijakan Politik Kriminal: Penegakan Hukum Dalam Rangka Penanggulangan Kejahatan. Pustaka Pelajar, 2010.

"Indra Safitri, 'Tindak Pidana Di Dunia Cyber', (Http://Business.Fortunecity.Com/Buffett/842/ Art180199_tindakpidana.Html), Diakses 15 Januari 2015.," n.d.

Iqbal, Muhamad, S. Suhendar, and Ali Imron. "Hukum Pidana," 2019.

"Kepala Biro Multimedia Mabes Polri Brigadir Jenderal Yan Fitri Halimansyah (Suara.Com/Maidian Reviani), Jum'at, 08 September 2017.," n.d.

Lamintang, P. A. F. "Dasar-Dasar Hukum Pidana Indonesia, Bandung: PT." Citra Aditya Bakti, 1997.

Marwin, Marwin. "Penanggulangan Cyber Crime Melalui Penal Policy." ASAS 5, no. 1 (2013).

Mayer, Jonathan. "Cybercrime Litigation." U. Pa. L. Rev. 164 (2015): 1453.

MEILANO, WAHYU. "PENERAPAN SANKSI PIDANA TERHADAP PELAKU TINDAK PIDANA POLITIK UANG PADA PEMILIHAN KEPALA DAERAH (STUDI KASUS PUTUSAN NOMOR: 238/PID. SUS/2018 PN. LHT)." PhD Thesis, Universitas Muhammdiyah Palembang, 2019.

ISSN: 2656-6141 (online)
Volume II Nomor 2 September 2020

Muladi, Diah Sulistyani. "Kompleksitas Perkembangan Tindak Pidana Dan Kebijakan Kriminal." Bandung: Alumni, 2016.

Peter Stephenson, 2000, Investigating Computer Telated Crime : A Handbook for Corporate Investigator, London, CRC Press, Hlm. 56., n.d.

Priatna, Mochamad Guruh Abdi, and R. A. S. Hernawati. "Tindak Pidana Penodaan Agama Oleh Pemeluknya Melalui Media Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Kitab Undang-Undang Hukum Pidana." Wacana Paramarta: Jurnal Ilmu Hukum 16, no. 3 (2017): 139–148.

Projodikoro, Wiryono. Asas-Asas Hukum Pidana Di Indonesia. Eresco, 1969.

Reinhardt, C. S., and Thomas D. Cook. "Beyond Qualitative versus Quantitative Methods." In Qualitative and Quantitative Methods in Evaluation Research, 7–32. Sage Publications, 1979.

Sigid Susone, Op.Cit., Hal. 198, n.d.

Soejadi, 2017, Refleksi Mengenai Hukum Dan Keadilan;; Aktualisasinya Di Indonesia, Aswaja Pressindo, Yogyakarta, Hal. 56-57., n.d.

Soekito, Sri Widoyati Wiratmo. Anak Dan Wanita Dalam Hukum. Lembaga Penelitian, Pendidikan dan Penerangan Ekonomi dan Sosial, 1983.

"Suara Merdeka, 'Situs Internet' (Http://Www.Suaramerdeka.Com/Harian/0207/24/Nas13. Html), Diakses 12 Januari 2015.," n.d.

Tongat, 2003, Hukum Pidana Materiil, Jakarta, Djambatan, Hlm. 24, n.d.

Wicaksono, Muhammad Friki. "PERANAN POLRI DALAM PENANGGULANGAN CYBER CRIME (Studi Kasus Di Polrestabes Semarang)." PhD Thesis, Fakultas Hukum UNISSULA, 2017.

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