ISSN 2656-4041 (Media Online)

PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA

Oleh :

Riko Nugraha
Universitas Dirgantara Marsekal Suryadarma Jakarta
Dosen Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma
Jl. Angkasa No. 1, Komplek Angkasa, Halim Perdanakusuma, Jakarta Timur
Email : rijko.nugraha@yahoo.com

Abstrak :
Kemajuan teknologi beserta penerapannya selalu mempunyai berbagai implikasi, baik bagi tatanan kehidupan sosial, bagi perkembangan dunia usaha, bagi perkembangan nilai-nilai Moral, Etika, maupun Hukum. Berikut akan diberikan gambaran tentang beberapa teknologi yang dianggap mampu mengubah peri kehidupan di dunia dalam segenap dimensinya.
Melalui teknologi multimedia maka jenis telekomunikasi menjadi sangat berkembang, tidak hanya meliputi telekomunikasi dasar, tetapi juga mencakup teknologi nilai tambah lainnya. Penetrasi internet yang begitu besar apabila tidak dipergunakan dengan bijak maka akan melahirkan kejahatan di dunia maya atau yang diistilahkan dengan kejahatan siber atau *cyber crime*[1] yang merupakan perkembangan lebih lanjut dari *computer crime*.
Tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi informasi. Di samping itu juga ditandai dengan adanya interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi.
Penanggulangan *cyber crime* oleh penegak hukum sangat dipengaruhi oleh adanya peraturan perundang- undangan, terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet yang diatur di dalam peraturan nasional.
Kata kunci : Kebijakan, Hukum Cyber, dan Penanganan Cyber di Indonesia, Peraturan PerUndang-Undangan.

Abstract :
The Technological of progression and application always have various of implications, well being for the order of social life, for the development of the business world, for the

[1] *Cyber crime* dapat didefinisikan bahwa*; "Cyber crime is used to refer both to traditional crimes (e.g extortion,*
fraud, forgery, identity theft, and child explotation) that are committed over electronic networks and information system as well as to crimes unique to electronic networks (e.g hacking and denial of service attacs). Also acts against confi dentiality, integrity and availability of data or system is the core of cyber crime" Terdapat 3 (tiga) kategori besar dari cyber crime, yaitu: 1) Computer Integrity Crime Terkait dengan integritas sistem komputer seperti hacking dan DDOS. 2) Computer Assisted Crime Perbuatan melawan hukum yang dibantu/memanfaatkan computer seperti: virtual robberies, scams, theft. 3) Computer Content Crime Perbuatan melawan hukum yang difokuskan pada isi (content) komputer, seperti pornografi dan komunikasi yang offensive. Dan lihat juga US Department of Homeland Security, American Cyber Security Enhancement Act of 2005.

development of moral, ethical, and legal values. The following will give an overview of some of the technologies that are considered capable of changing the fairy life in the world in all its dimensions.
Through multimedia of technology, the type of telecommunications has become highly developed, Close only the covering basic telecommunications, but also including other value-added technologies. Internet penetration is so large if not used wisely it will give birth to crime in cyberspace or what is termed cyber crime or cyber crime which is a further development of computer of crime.
Information technology crime is a relatively new form of crime when compared to other forms of crime that are conventional in nature. Information technology crimes emerged simultaneously with the birth of the information technology revolution. In addition, it is also marked by social interactions that minimize physical presence, which is another characteristic of the information technology revolution.
Prevention of cyber crime by law enforcement is strongly influenced by the existence of laws and regulations, there are several laws relating to information technology, especially crimes related to the internet which are regulated in national regulations.

Keywords: Policy, CyberLaw, and The Indonesia Cyber of Handling, National Regulation.

A. Pendahuluan

1. Latar Belakang

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi[2] yang berlangsung hampir di semua bidang kehidupan manusia. Revolusi yang dihasilkan oleh teknologi informasi dan komunikasi biasanya dilihat dari sudut pandang penurunan jarak geografis, penghilangan batas-batas negara dan zona waktu serta peningkatan efisiensi dalam pengumpulan, penyebaran, analisis dan mungkin juga penggunaan data.

Disamping berbagai hal positif yang diapat diambil dari kemajuan teknologi informasi dan transaksi

[2] Perkembangan teknologi yang sangat pesat di bidang ICT dan bidang-bidang lain yang terkait akan menimbulkan tantangan-tantangan baru. Tantangantantangan baru tersebut diakibatkan oleh ciri-ciri dari teknologinya yang mempunyai jangkauan global (*borderless and unbounded);* sifat anonymity dari pelaku tertentu (misalnya *cyber criminals*) yang cenderung menyembunyikan identitas yang sesungguhnya. Kemudian juga sifat asimetri dari teknologi yang dimediasi oleh jaringan dan teknologi informasi. Masalah cyber security telah menjadi perhatian serius, baik pada level internasional maupun nasional. Dalam lingkup nasional bentukbentuk ancaman terhadap cyber security Perkembangan teknologi dan penerapannya tersebut, tidak hanya mengubah wajah bisnis secara revolusioner, namun juga menimbulkan perubahan dalam Tatanan Sosial, Moral, Etika dan Hukum. Nilai-nilai baru yang dihadirkan tentu saja tidak selalu sama dengan nilai-nilai sebelumnya, bahkan berpotensi menimbulkan konfl ik nilai yang perlu dicermati dan dicari jalan keluarnya, terutama dari perspektif Etika dan Hukum. Bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangs. Dan lihat juga UU No. 19 Tahun 2019 Tentang Perubahan atas Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik serta Undang-Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik.

elektronik komunikasi, perkembangannya yang pesat dari perkembangan internet juga menimbulkan pro dan kontra. Prinsipnya, internet membuat kejahatan yang semula bersifat konvensional dan langsung seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak pidana terorisme kini melalui media internet beberapa jenis tindak pidana tersebut dapat dilakukan secara online oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun Negara.[3]

Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi informasi. Di samping itu juga ditandai dengan adanya interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi.[4]

Penetrasi internet yang begitu besar apabila tidak dipergunakan dengan bijak maka akan melahirkan kejahatan di dunia maya atau yang diistilahkan dengan kejahatan siber atau *cyber crime*[5] yang merupakan perkembangan lebih lanjut dari *computer crime*. Dunia maya (*cyberspace*) saat ini ternyata rentan terhadap perilaku kriminal. Sebagai contoh adalah praktik- praktik implantasi virus yang mencederai komputer di seluruh dunia, bank dan lembaga keuangan telah kehilangan uang dalam jumlah besar. Negara maju seperti Amerika Serikat dan Inggris dan beberapa negara lainnya mengungkapkan bahwa data tentang keamanan nasional telah dibobol dan di download oleh orang-orang yang tidak berkepentingan. Tindak pidana lain juga dapat dilakukan melalui media internet seperti pornografi anak, penyerangan terhadap privacy seseorang, perdagangan barang ilegal, atau hadirnya situs-situs yang meresahkan masyarakat. Contoh lain, bagi mereka yang senang akan perjudian dapat melakukannya dari rumah atau di kantor.

2. Perumusan Masalah

Sebagaimana telah diuraikan di atas bahwa Cyber Law sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana. Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer,

[3]Golos P. R.., "Penegakan Hukum *Cybercrime dalam Sistem Hukum Indonesia dalam Seminar Pembuktian dan Penangan Cybercrime* di *Indonesia".2007. hlm. 12.*

[4] Nitibaskara, Tubagus Ronny Rahman. *Ketika kejahatan berdaulat: sebuah pendekatan kriminologi, hukum dan sosiologi*. 2011. hlm. 31

[5] *Cyber crime* dapat didefinisikan bahwa*; "Cyber crime is used to refer both to traditional crimes (e.g extortion,*
fraud, forgery, identity theft, and child explotation) that are committed over electronic networks and information system as well as to crimes unique to electronic networks (e.g hacking and denial of service attacs). Also acts against confi dentiality, integrity and availability of data or system is the core of cyber crime" Terdapat 3 (tiga) kategori besar dari cyber crime, yaitu: 1) Computer Integrity Crime Terkait dengan integritas sistem komputer seperti hacking dan DDOS. 2) Computer Assisted Crime Perbuatan melawan hukum yang dibantu/memanfaatkan computer seperti: virtual robberies, scams, theft. 3) Computer Content Crime Perbuatan melawan hukum yang difokuskan pada isi (content) komputer, seperti pornografi dan komunikasi yang offensive. Dan lihat juga US Department of Homeland Security, American Cyber Security Enhancement Act of 2005.

termasuk kejahatan pencucian uang dan kejahatan terorisme dan lain sebagainya.

Memperhatikan uraian pada latar belakang sebagaimana diuraikan di atas, permasalahan dalam penelitian ini dirumuskan, sebagai berikut;

1. Bagaimana kebijakan terhadap pelaksanaan *Cyberlaw* di Indonesia?
2. Bagaimanakah upaya pemeritah terhadap penanganan *Cyberlaw* dimasa yang akan datang?

3. Tujuan dan Manfaat Penelitian

Berdasarkan latar belakang dan pokok permasalahan di atas, tujuan dan manfaat penelitian adalah sebagai berikut;

Tujuan Penelitian;

1. Untuk mengetahui faktor-faktor apa saja yang mendominanasi dalam rangka mengetahui kebijakan dan hukum C*yberlaw* di Indonesia.
2. Upaya apa saja yang perlu dilaksanakan dalam rangka pengantisipasian perubahan penyelenggaraan usaha telekomunikasi sejalan dengan prinsip dalam upaya pemeritah terhadap penanganan *Cyberlaw* dimasa yang akan datang.

Manfaat Penelitian;

1. Penelitian ini dapat memberikan kontribusi pemikiran dalam rangka pengembangan khasanah ilmu pengetahuan khususnya dibidang hukum *Cyberlaw* dan Informasi Teknologi dan Telekomunikasi (ITE).
2. Bahwa hukum *cyberlaw* dan telekomuniasi dapat dijadikan sebagai landasan hukum, rujukan dan/atau references sesuai ketentuan hukum *cyberlaw* dan Informasi Teknologi dan Telekomunikasi (ITE).

Manfaat Praktis:

1. Penelitian ini diharapkan dapat memberikan masukan-masukan kepada regulator khususnya dalam bidang *cyberlaw,* Informasi Teknologi dan Telekomunikasi (ITE).
2. Penelitian ini berguna untuk menambah wawasan dengan memberikan gambaran bagi pembaca terutama di bidang *cyberlaw* dan Informasi Teknologi dan Telekomunikasi (ITE) baik para Penganjar (Dosen), mahasiswa fakultas hukum maupun masyarakat luas.

C. PENELITIAN DAN PEMBAHASAN

1. Kebijakan dan Hukum Siber di Indonesia dalam Menaggulanginya

Dalam menanggulangi kejahatan *Cyber* maka diperlukan adanya hukum *Cyber* atau *Cyber Law*. *Cyber Law* adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet / elektronik yang dimulai pada saat mulai "online" dan memasuki dunia *cyber* atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju.

Jonathan Rosenoer (1997) membagi ruang lingkup *Cyber Law* dalam beberapa hal diantaranya: *Copy right* (hak cipta), *Trademark* (hakmerek), *Defamation* (penc emaran nama baik), *Hate Speech* (penistaan, penghinaan, fitnah), *Hacking, Viruses, Illegal Access*, (penyerangan terhadap computer / Optik lain), *The Regulation Internet* of *Resource*

(pengaturan / *Regeling* sumber daya internet), *Privacy* (kenyamanan pribadi), *Duty Care* (kehati - hatian), *Criminal Liability* (kejahatan / *Criminal* dengan menggunakan Informasika dan Teknologi), *Procedural Issues* (yuridiksi, pembuktian, penyelidikan, dll.), *Electronic Contract* (transaksi elektronik), *Pornography*, *Robbery* (pencurian lewat internet), *Consumer Protection* (perlindungan konsumen), dan *E-Commerce, E-Government* (pemanfaatan internet dalam keseharian).

Cyber Law sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, maupun penanganan tindak pidana. Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan - kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.

Cyber Law penting diberlakukan sebagai hukum di Indonesia. Hal tersebut disebabkan oleh perkembangan zaman. Menurut pihak yang pro terhadap *Cyber Law*, sudah saatnya Indonesia memiliki *Cyber Law*, mengingat hukum - hukum tradisional tidak mampu mengantisipasi perkembangan dunia maya yang pesat.

Salah satu contoh kasus dalam kejahatan *cyber* adalah kasus yang dialami oleh Wakil Ketua MPR periode 2009-2014 Lukman Hakim Saifuddin, di mana *e-mail* beliau dibajak oleh seseorang untuk mendapatkan kepentingan dengan sejumlah uang dengan mengirimkan surat kepada kontak-kontak yang ada di *e-mail* milik beliau. Lukman Hakim Saifuddin memiliki hak sebagaimana diatur dalam Pasal 26 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") yang mengatakan bahwa "setiap orang yang dilanggar haknya sebagaimana yang dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Dengan hak yang telah disebutkan di atas, Lukman Hakim Saifuddin berhak untuk mengajukan gugatan yang berdasarkan pada Pasal 28 ayat (1) UU ITE yang berbunyi, "setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik", di mana hal tersebut merupakan perbuatan yang dilarang.

Sejalan dengan itu, pelaku dapat dikenakan pidana sesuai ketentuan Pasal 45A[6] UU ITE yang berbunyi, *"Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik'* sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Dalam kasus yang menimpa Lukman Hakim Saifuddin tersebut, pelaku kejahatan dunia maya yang membajak *e-mail* beliau juga dapat diterapkan dengan pelanggaran Pasal

[6] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

378 KUHP tentang penipuan yang berbunyi, "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (*hoendanigheid*) palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, mengerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun.

Dalam bacground paper untuk lokakarya konfrensi PBB X/2000 di Wina, Austria, istilah cybercrime dibagi dalam dua kategori, yaitu pertama, cyber crime dalam arti sempit disebut computer crime, kedua cybercrime dalam arti luas disebut *computer related crime*. Dalam dokumen tersebut dinyatakan: *a. Cybercrime in narrow sanse (computer crime): any legal behaviour directed by means of elctronik operations that targets the security of computer system and data procssed by them. b. Cybercime in a broader sense (computer related crime): any ilegal behaviour commited by means on in reltion to, a computer systemor network, including such crime as illegal possesion, offering or distribution by meaans of a computer system or network*.[7] Dengan menggunakan sarana - sarana dari sistem atau jaringan komputer (*by means of a computer system or network*) Didalam sistem atau jaringan komputer (in a computer system or network) dan 3. Terhadap sistem atau jaringan komputer (*ageinst a computer system or network*). Dari defenisi tersebut, maka dalam arti sempit cyber crime adalah computer crime yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, cyber crime mencakup seluruh bentuk baru kejahatan yang ditujukan kepada komputer, jaringan komputer dan penggunanya serta bentuk-bentukk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime*).

Transaksi elektronik adalah perbuatan hukum yang dilakukan melalui komputer, jaringan komputer atau media elektronik lainnya.[8] Lebih lanjut yang dimaksud dengan komputer adalah alat proses data elektronik, mengetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika dan penyimpanannya. Berdasarkan pengertian tersebut, maka transaksi elektronik memiliki cakupan yang sangat luas, baik mengenai subyeknya yaitu tiap orang pribadi atau badan yang yang memanfaatkan yang memanfaatkan komputer, jaringan komputer atau media elektronik lainnya, maupun mengenai obyeknya yang meliputi berbagai barang dan jasa. Dalam implementasinya, transaksi elektronik dilakukan dengan menggunakan *interconected network* (internet), yaitu jaringan komputer yang terdiri dari berbagai macam ukuran jaringan yang saling dihubungkansatu sama lain lewat

[7] Laporan Konfrensi PBB X/2000, : *The term computer related crime had been developed to encompass both the entirely new forms of crime that were directed at computers, net work and their users, and the more traditional form of crime that were now being commited whit use or assistence of computer aquipment*, dalam Barda Nawawi Arif, 2001, *Masalah Penegakkan Hukum & Kebijakan Penanggulangan Kejahatan*, Ctra Aditya Bakti, Bandung, hlm.249-250.

[8] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik.*

suatu medium komunikasi secara elektronik dan dapat saling mengakses semua layanan (*services)* yang disediakan oleh jaringan lainnya[9].

Dalam kaitan dengan upaya pencegahan tindak pidana, ataupun penangan tindak pidana, UU ITE akan menjadi dasar hukum dalam proses penegakan hukum kejahatan-kejahan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.[10]

Berikut ini akan diuraikan faktor-faktor yang mempengaruhi penegakan hukum terhadap kejahatan siber (*ciber crimes*). Faktor-faktor yang dimaksud yaitu penegakan hukum terhadap kejahatan siber sangat dipengaruhi oleh faktor hukum. Karena kejahatan siber berada pada anatomi kejahatan transnasional maka hukum yang digunakan adalah hukum nasional yang dalam pembahasan ini adalah hukum Indonesia. Namun sepanjang tidak diatur dalam hukum nasional maka yang dipergunakan adalah asas-asas, prinsip – prinsip dan kaidah hukum internasional.

Penanggulangan *cyber crime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang - undangan, terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet sebelum disahkannya UU ITE. Penegakkan hukum cybercrime sebelum disahkannya UU ITE dilakukan dengan menafsirkan *cyber crime* ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi diantaranya:

a) Undang – Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik;
b) Undang -Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
c) Undang-Undang No. 19 tahun 2002 sebagaimana telah diubah oleh Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta;
d) Undang-Undang No. 25 Tahun 2003 tentang Perubahan atas Undang – Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang sebagaimana telah diganti dengan Undang-Undang No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
e) Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme;
f) Dan lain sebagainya.

Dalam perkembangannya, pengaturan cyber space dan kejahatan siber (ciber crimes) diatur di dalam Undang - undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sebagai payung hukum. UU ITE ini diharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan

[9] Daniel H Purwadi, *Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia*, PT Elex Media Komputindo, Jakarta 1995, hlm.1.

[10] T. Nasrullah, *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan* : Jakarta Raya.,2003:hlm.,3.

internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.

Pada dasarnya, Undang – undang ini telah memenuhi syarat keberlakuan hukum baik secara yuridis, sosiologis dan filosofis. Secara filosofis, lahirnya Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Eleketronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik didasarkan amanat yang terkandung pada Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945.[11] yang menyatakan. Secara yuridis, undang- undang ini telah mengatur mengenai segala sesuatu yang berkaitan dengan kegiatan internet, perangkat komputer, dan instrumen elektronik lainnya. Secara sosiologis, masyarakat memang memerlukan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik untuk mengatur berbagai aktivitas yang mereka lakukan selama berinteraksi di *cyber space*. Dinamika globalisasi informasi telah menuntut adanya suatu aturan untuk melindungi kepentingan para netter dalam mengakses pelbagai informasi. Pengaturan dalam Undang - undang Nomor 11 Tahun 2008.

Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang – Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini sejalan dengan agama, nilai-nilai maupun kaidah moral yang diterima secara universal sehingga keberadaan cyber law (termasuk instrumen hukum internasional yang mengaturnya) diakui, diterima dan dilaksanakan oleh *information society*.

Dalam praktik penegakan hukum terhadap apapun bentuk kejahatan-kejahatan transnasional salah satunya kejahatan siber (*cyber crimes)*, faktor hukum yang utama yang seringkali menjadi kendala penegakan hukum dalam praktik adalah masalah yurisdiksi. Masalah keraguan penentuan yurisdiksi dalam cyber space pun justru diakui oleh pakar hukum itu sendiri. Tien S. Saefullah yang menyatakan bahwa yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian kovensional, didasarkan pada batas-batas geografis dan waktu sementara komunikasi dan informasi multimedia bersifat internasional, multi yurisdiksi dan tanpa batas – batas geografis sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia dewasa ini sebagai salah satu pemanfaatan teknologi informasi.[12]

Penentuan yurisdiksi merupakan suatu diskursus yang sangat penting dalam rangka penegakan *cyber law* apalagi dalam konsteks penegakan

[11] Pasal 28F UUD 1945 bahwa Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

[12] Mansur, Dikdik M. Arief. *Cyber Law: Aspek Hukum Teknologi Informasi*. Tiga Serangkai, 2007. hlm.34.

hukum terhadap kejahatan transnasional. Permasalahan mengenai yurisdiksi diatur dalam Pasal 2 Undang – undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang – Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan Undang – Undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang - undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Selanjutnya, dalam Pasal 1 angka 21 yang menyatakan bahwa "orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum."

Dalam penjelasan Pasal 2 disebutkan Undang - Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/ atau 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. Yang dimaksud dengan "merugikan kepentingan Indonesia adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

"Darrel Menthe menyatakan bahwa yurisdiksi di *cyber space* membutuhkan prinsip - prinsip yang jelas yang berakar dari hukum internasional. Hanya melalui prinsip-prinsip yurisdiksi dalam hukum internasional ini, negara-negara kiranya dapat mengadopsi pemecahan yang sama terhadap pertanyaan mengenai yurisdiksi internet.[13] Pendapat Menthe ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip yurisdiksi yang berlaku dalam hukum internasional dalam kegiatan cyber space oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi *cyber crime*. Pada hakikatnya untuk menentukan yurisdiksi manakah yang dapat diterapkan dalam kegiatan cyberspace, termasuk di dalamnya cyber crime, tidak perlu dicari yurisdiksi tertentu yang lain dari pada yang lain (yurisdiksi dengan karakteristik khusus), karena sebenarnya prinsip - prinsip dalam hukum internasional sudah memadai untuk dipergunakan.[14]

"Penentuan yurisdiksi *cyber crimes* dapat ditelaah dari asas-asas hukum internasional. Ada dua pandangan dari negara yakni perundang – undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di dalam wilayah negara, baik dilakukan oleh warga negaranya sendiri maupun oleh orang asing

[13] *Ibid*.,hlm.37
[14] *Ibid.,* hlm.38

(asas teritorial). Kedua, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara, dimana saja, juga di lua wilayah negara (asas personal). Juga dinamakan prinsip nasionalitas yang aktif. Lebih lanjut dikatakan bahwa dasar lain yang masuk akal bahwa hukum pidana di luar negara adalah asas melindungi kepentingan. Ini dapat dibedakan antara melindungi kepentingan nasional (prinsip nasional pasif) dan melindungi kepentingan internasional (prinsip universal).

Dalam substansi hukum di Amerika terdapat beberapa teori yang berkaitan dengan yurisdiksi di *cyber space* yakni:[15]

a. *The theory of the uploader and the downloader* (teori tentang mengunggah dan mengunduh).

   Uploader (pengunggah) adalah pihak yang memasukkan informasi elektronik ke dalam cyber space sedangkan downloader (pengunduh) adalah pihak yang mengakses Informasi. Pada umumnya, yurisdiksi mengenai perbuatan-perbuatan perdata dan tindak pidana tidak ada kesulitan. Suatu negara dapat melarang dalam wilayahnya kegiatan uploading dan downloading yang diperkirakan dapat bertentangan dengan kepentingan negaranya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian dalam wilayah negaranya dan melarang setiap orang dalam wilayahnya untuk downloading kegiatan perjudian.

b. *The theory of the law of the server* (teori hukum pusat penyedia).

   Pendekatan lain yang dapat digunakan adalah memperlakukan server dimana webpages secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang berlokasi di server pada Standford University tunduk pada hukum California. Namun teori ini akan sulit dipergunakan apabila uploader berada dalam yurisdiksi asing.

c. *The theory of International Space*

   (teori ruang internasional). Menurut teori ini, cyber space adalah lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama. Dalam kaitan dengan teori ini Menthe mengusulkan agar cyber space menjadi fourth space. Yang menjadi dasar analogi tidak terletak pada kesatuan fisik, melainkan pada sifat internasional yakni sovereignless quality (kualitas kedaulatan). Semua kegiatan dalam *cyber space* dianalogikan dengan kegiatan ruang angkasa. Semua kegiatan ini diatur secara bersama – sama.

   Bahwa dalam melakukan penanganan pelanggaran UU ITE, penegak hukum diminta memedomani hal-hal seperti, mengikuti perkembangan pemanfaatan ruang digital yang terus berkembang dengan segala macam persoalannya; memahami budaya beretika yang terjadi di ruang digital dengan menginventarisasi berbagai permasalahan dan dampak yang

[15] Saefullah, Tien S. "Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar." *Pusat Studi Cyberlaw Fakultas Hukum UNPAD. ELIPS* (2009).hlm. 102-103

terjadi di masyarakat; mengedepankan upaya preemtif dan preventif melalui virtual police dan virtual alert yang bertujuan untuk memonitor, mengedukasi, memberikan peringatan, serta mencegah masyarakat dari potensi tindak pidana siber. Pada dasarnya penerapannya dalam menerima laporan dari masyarakat, penyidik harus dapat dengan tegas membedakan antara kritik, masukan, hoaks, dan pencemaran nama baik yang dapat dipidana untuk selanjutnya menentukan langkah yang akan diambil. Sejak penerimaan laporan, penyidik berkomunikasi dengan para pihak terutama korban (tidak diwakilkan) dan memfasilitasi serta memberi ruang seluas-luasnya kepada para pihak yang bersengketa untuk melaksanakan mediasi. Melakukan kajian dan gelar perkara secara komprehensif terhadap perkara yang ditangani dengan melibatkan para penegak hukum/apparat penegak hukum secara kolektif kolegial berdasarkan fakta dan data yang ada.

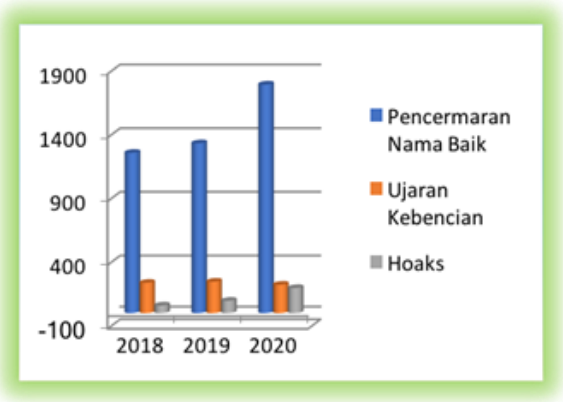
Upaya terakhir dalam penegakan hukum (*ultimatum remidium*)[16] dan mengedepankan *restorative of justice* dalam penyelesaian perkara; Terhadap para pihak dan/atau korban yang akan mengambil langkah damai agar menjadi bagian prioritas penyidik untuk dilaksanakan *restorative of justice* terkecuali perkara yang bersifat berpotensi memecah belah, SARA, radikalisme, dan separatism.

Berikut data rekapitulasi kasus *cyber crime* di Indonesia;[17]

Gambar 1. Persentase *Cyber Crime* di Indonesia, pada Tahun 2018 itu ada laporan polisi 4.360. Kemudian 2019 meningkat jadi 4.586. Kemudian 2020 meningkat lagi menjadi 4.790. Ini kecenderungannya laporan polisi terkait UU ITE meningkat.

[16] *Ultimum remedium* merupakan salah satu asas yang terdapat dalam hukum pidana Indonesia. *Ultimum remedium* merupakan salah satu asas yang terdapat di dalam hukum pidana Indonesia yang mengatakan bahwa hukum pidana hendaklah dijadikan upaya terakhir dalam hal penegakan hukum. ultimum remedium ini berprinsip yang berada di tengah-tengah moral dan hukum, yang kedua adalah ultimum remedium itu merupakan prinsip segala proses legislasi. Jadi bagaimana menolak kriminalisasi atau negoisasi maka ultimum remedium menjadi patokannya, bukan ketika kita menegakan hukum kalau Undang-undang sudah ada, pasal sudah ada maka polisi atau jaksa tentu tidak bisa menggunakan prinsip ini. *Ultimum remedium* merupakan istilah lumrah yang kemudian biasa dipakai atau dikaitkan dengan hukum. Istilah ini menggambarkan suatu sifat hukum, yakni sebagai pilihan atau alat terakhir yang dikenal baik dalam hukum pidana. Lihat juga Prof. Topo Santoso, S.H., M.H., Ph.D. *Ultimatum Remedium; Antara Prinsip Moral dan Prinsip* Hukum. Guru Besar Uiniversitas Indonesia. FH-UI. Jakarta. Indonesia. 2019.

[17] Data diambil dan diolah dari Direktorat Reserse Kriminal Khusus, *Cyber Law*. Di Jakarta. Indonesia. Dari tahun 2018 – 2020. Data diambil pada Senin, 21 Juni 2021.



Gambar 2. Diagram Bentuk Cyber Crime di atas dapat kita lihat bahwa cenderung mengalami peningkatan. Kasus pencemaran nama baik masih mendominasi laporan di kepolisian terkait UU ITE. Pada tahun 2018 terdapat 1.258 laporan, 2019 sebanyak 1.333 laporan dan pada 2020 menjadi 1.794 laporan polisi yang menyangkut pencemaran nama baik. Urutan kedua ditempati ujaran kebencian sebanyak 238 laporan pada 2018, meningkat mencapai 247 laporan pada 2019 dan 223 laporan polisi pada 2020. Selanjutnya terkait informasi hoaks atau kabar bohong juga mengalami hal serupa. "2018 itu 60 kasus, 2019 ada 97 kasus, dan 2020 menjadi 197 kasus yang menyangkut hoaks.

2. Upaya Penanggulangan Kejahatan Siber Di Indonesia

Belum optimalnya penegakan hukum terhadap *cyber crimes* disebabkan karena sarana dan fasilitas penegakan hukum yang belum memadai. Penegakan hukum terhadap cyber crimes mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud. Penentuan waktu dan tempat terjadinya cyber crimes ditentukan saat kapan alat itu bekerja efektif, oleh sebab itu analisis telematika sangat diperlukan dalam mengungkap kejahatan ini. Untuk menelusi, mendeteksi dan menanggulangi kejahatan ini Onno W. Purbo menjelaskan bahwa caranya sangat tergantung aplikasi dan topologi jaringan yang dipakai. Sebagian aplikasinya ada di gnacktrack dan backtrack. Hal ini menggambarkan bahwa sarana dan fasilitas yang memadai menjadi hal yang penting dalam proses penegakan hukum. Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapai tujuannya.

Untuk meningkatkan upaya penanggulangan kejahatan siber atau cyber crimes yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan cyber dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personelnya ke berbagai macam kursus yang berkaitan dengan cyber crime. Pengiriman personel Polri tidak hanya terbatas dilakukan dalam lingkup nasional tetapi juga dikirim untuk mengikuti kursus di negara-negara maju agar dapat diterapkan dan diaplikasikan di Indonesia.

Pelatihan, kursus dan ceramah kepada aparat penegak hukum lain (misalnya Jaksa dan Hakim) mengenai cyber crime juga hendaknya dilaksanakan, dikarenakan Jaksa dan Hakim belum memiliki satuan unit khusus yang menangani kejahatan dunia maya sehingga diperlukan sosialisasi terutama setelah disahkannya UU ITE agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan terhadap kejahatan siber. Jaksa dan Hakim cyber sangat dibutuhkan seiring dengan perkembangan tindak pidana teknologi yang semakin banyak terjadi di masyarakat yang akibatnya dapat dirasakan di satu daerah, di luar daerah perbuatan yang dilakukan bahkan di luar negeri. Kurangnya sarana dan prasarana dalam penegakan hukum cyber crime, sangat berpengaruh terhadap kinerja aparat penegak hukum dalam menghadapi high tech crimes.

Pencegahan dan penanggulangan terhadap cyber crimes membutuhkan pendekatan penal dan non penal yang integral dan membutuhkan keterpaduan. Membicarakan masyarakat adalah suatu keharusan atau kewajiban yang melekat pada perbincangan mengenai hukum. Hukum dan masyarakatnya merupakan dua sisi dari satu mata uang. Maka tanpa perbincangan mengenai masyarakat terlebih dahulu, sesungguhnya berbicara tentang hukum yang kosong.[18]

Satjipto Rahardjo menyimpulkan bahwa "setiap anggota masyarakat sebagai pemegang peranan ditentukan tingkah lakunya oleh pola-pola peraturan yang diharapkan daripadanya baik oleh norma – norma hukum maupun oleh kekuatan-kekuatan di luar hukum." Penegakan hukum berasal dari masyarakat dan bertujuan untuk mencapai kedamaian di dalam masyarakat. Oleh karena itu, dipandang dari sudut tertentu, maka masyarakat dapat mempengaruhi penegakan hukum tersebut. Pengaruh masyarakat dalam penegakan hukum ini ditelaah dari kesadaran hukum yang menjadi indikator dari derajat kepatuhan hukum.

Kesadaran hukum masyarakat sangat diperlukan dalam berteknologi dan rendahnya kesadaran hukum para netter menjadikan penegakan hukum terhadap cyber crimes tidak berjalan optimal. Tidak adanya kesadaran hukum para netter ini terlihat pada pemanfaatan sarana internet untuk melakukan berbagai jenis tindak pidana salah satunya memperjualbelikan layanan seks dan berbagai jenis tindak pidana lainnya.

Kesadaran hukum dari para korban untuk melaporkan kejahatan yang dialaminya masih sangat sedikit. Berdasarkan laporan Symantec bertajuk Norton Cybercrime Report, hampir satu dari dua (45 persen) korban kejahatan siber (cyber crimes) tidak pernah menyelesaikan secara tuntas kejahatan cyber yang mereka alami. Padahal, sebanyak 86 persen pengguna yang disurvei mengaku pernah menjadi korban pelaku kejahatan tindak pindana cyber.[19] Korban dari kasus eksploitasi seksual pun jarang ada yang melaporkan, hal ini disebabkan karena korban malu apabila ada

[18] Rahardjo, Satjipto. *Hukum dan Perilaku: hidup baik adalah dasar hukum yang baik.* Penerbit Buku Kompas, 2009.hlm.9.

[19] http://teknologi.vivanews.com/news/read/180241-45--korban-cybercrime-tak- melapor diakses pada tanggal 8 Juli 2021.

orang yang mengetahui kejadian yang dialaminya.

Kurangnya kesadaran hukum masyarakat berimplikasi dan pemahaman serta ketidaktaatan mereka terhadap hukum. Dikdik M. Arief Mansur dan Elisatris Gultom merumuskan beberapa alasan maka sampai saat ini kesadaran hukum masyarakat Indonesia masih sangat kurang, yakni: Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas cyber crime masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (lack of information) masyarakat terhadap jenis kejahatan cyber crime. Lack of information ini menyebabkan upaya penanggulangan cyber crime mengalami kendala, dalam hal ini kendala yang berkenaan dengan penaatan hukum dan proses pengawasan (controlling) masyarakat terhadap setiap aktivitas ang diduga berkaitan dengan cyber crime. Dengan demikian, kiranya tepatlah jika dikatakan bahwa penegakan hukum yang optimal memerlukan kesadaran hukum dan kesadaran moral dari masyarakat.

D. KESIMPULAN

Mengenai penanganan *cyberlaw* di Indonesia, maka dapat disimpulkan beberapa hal, sebagai berikut:

a. Modus operasi cybercrime sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan – kejahatan konvensional. Perbedaan utamanya adalah bahwa cybercrime melibatkan komputer dalam pelaksanaannya. Kejahatan - kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatankejahatan ini memiliki karakter yang berbeda dari kejahatan – kejahatan konvensional
b. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.
c. Hambatan – hambatan yang ditemukan dalam upaya melakukan penyidikan terhadap *cyber crime* terkait dengan undang-undang ITE antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyidikan terhadap cybercrime antara lain berupa penyempurnaan perangkat hukum, mendidik para penyidik, membangun fasilitas forensic computing, meningkatkan upaya penyidikan dan kerja sama nasional dan internasional, serta melakukan upaya penanggulangan pencegahan.

DAFTAR PUSTAKA

Buku-Buku

Barda Nawawi Arif, 2001, *Masalah Penegakkan Hukum & Kebijakan Penanggulangan Kejahatan,* Ctra Aditya Bakti, Bandung,

Daniel H Purwadi, *Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia*, PT Elex Media Komputindo, Jakarta 1995,

Edmon, Makarim,. Komplikasi Hukum Telematika. Jakarta: RajaGrafindo. 2003.

Golos P. R, "Penegakan Hukum *Cybercrime* dalam sistem Hukum Indonesia dalam seminar Pembuktian dan Penanganan *Cybercrime* di Indonesia". 2007.

Nasrullah, *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan* : Jakarta Raya.,2003

Nitibaskara, Tubagus Ronny Rahman. *Ketika kejahatan berdaulat: sebuah pendekatan kriminologi, hukum dan sosiologi*. 2011

Mansur, Dikdik M. Arief. *Cyber Law: Aspek Hukum Teknologi Informasi*. Tiga Serangkai, 2007.

Rafiqul Islam, Interntional Trade Law, London ; LBC, 1999

Rahardjo, Satjipto. *Hukum dan Perilaku: hidup baik adalah dasar hukum yang baik*. Penerbit Buku Kompas, 2009.

Romli, Atmasasmita, Terori Kapita Selekta Kriminologi. Bandung: Refika Aditama. 2005.

Saefullah, Tien S. "Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar." *Pusat Studi Cyberlaw Fakultas Hukum UNPAD. ELIPS* (2009).

US Department of Homeland Security, American Cyber Security Enhancement Act of 2005.

Peraturan PerUndang-undangan;

Undang-Undang Dasar 1945

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik