# UPAYA PENCEGAHAN ATAS PENYALAHGUNAAN *VIRTUAL PRIVATE NETWORK* (VPN) BERDASARKAN HUKUM POSITIF DI INDONESIA

**ACHMAD BACHTIAR RACHMAN**
21501021019

Fakultas Hukum
Universitas Islam Malang
Jln. MT Haryono 193 Dinoyo Kota Malang, 65144

## ABSTRAK

Seiring perkembangan zaman perkembangan teknologi informasi dapat memudahkan manusia untuk mengetahui informasi dari seluruh dunia melalui internet. Dengan mudahnya internet kita bisa melihat informasi dari seluruh dunia dengan sangat mudah. Dengan munculnya internet telah membawa sebuah dunia baru bagi seluruh dunia termasuk Indonesia. Kemajuan teknologi juga membuat perubahan dalam kehidupan bermasyarakat, terutama dalam nilai-nilai sosial.

Penelitian hukum berjudul: Upaya Pencegahan Atas Penyalahgunaan *Virtual Private Network* (VPN), jenis penelitian ini menggunakan penelitian normatif yang dimaksudkan menggunakan adalah metode atau cara meneliti bahan pustaka yang bersifat deskriptif yakni untuk pemecahan masalah yang ada pada masa sekarang sehingga bisa menemukan solusi untuk mengatasi permasalahan yang terjadi pada saat ini.

Berdasarkan dari hasil penelitian dan pembahasan peneliti menyimpulkan bahwa untuk kejahatan yang ditimbulkan *Virtual Private Network* (VPN) seperti penipuan dan pencurian data, hal ini dikarenakan ketika menggunakan VPN maka identitas kita tidak dapat muncul. Hambatan-hambatan juga terdapat dalam upaya melakukan pencegahan penanggulangan *Virtual Private Network* (VPN) diantaranya seperti barang bukti mudah dihilangkan dan kemampuan penegak hukum yang menguasai bidang teknologi terbatas. Dalam Pasal 40 (2a) dan (2b) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjelaskan bahwa pemerintah wajib melakukan pencegahan dari segala muatan yang dilarang oleh undang-undang dan pemerintah juga berwenang melakukan pemutusan akses.

Kata Kunci: Pencegahan, Hukum, VPN

## ABSTRACT

Along with the development of the times the development of information technology can make it easier for humans to know information from all over the world through the internet. With the ease of the internet we can see information from all over the world very easily. With the advent of the internet, it has brought a new world to the whole world including Indonesia. Technological advances also make changes in social life, especially in social values.

Legal research entitled: Prevention of Abuse of Virtual Private Networks (VPN), this type of research uses normative research that is intended to use is a method or method of researching library materials that are descriptive, namely to solve existing problems in the present so they can find solutions to overcome problems that happened at this time.

Based on the results of the research and discussion the researchers concluded that for crimes caused by Virtual Private Networks (VPN) such as fraud and data theft, this is because when using a VPN, our identity cannot appear. Barriers also exist in efforts to prevent the prevention of Virtual Private Networks (VPN) such as evidence that is easily removed and the ability of law enforcers who control the technology field is limited. In Articles 40 (2a) and (2b) of the Law of the Republic of Indonesia Number 19 Year 2016 concerning Amendments to Law Number 11 Year 2008 concerning Information and Electronic Transactions, it is explained that the government is obliged to prevent all contents prohibited by law and the government is also authorized to terminate access.



Keywords: Prevention, Law, VPN

# I. PENDAHULUAN

## A. Latar Belakang Masalah

Seiring perkembangan zaman perkembangan teknologi informasi dapat memudahkan manusia untuk mengetahui informasi dari seluruh dunia melalui internet. Dengan mudahnya internet kita bisa melihat informasi dari seluruh dunia dengan sangat mudah. Semua orang dari berbagai kalangan bisa mengakses internet tanpa takut dengan biaya yang mahal, hal ini dikarenakan banyak ditemukan akses WI-FI gratis yang bisa menghubungkan internet.

Indonesia adalah salah satu negara di Asia Tenggara yang memiliki pengguna internet terbesar. Pada tahun 2013, berdasarkan *Digital Landscape* di Indonesia yang diambil berdasarkan data dari Kemenkominfo, AAPJI dan survey dari Adplus menunjukkan bahwa orang Indonesia mengakses internet atau online selama 35 jam per minggu.[1] Internet di Indonesia memiliki perkembangan dan pertumbuhan yang sangat pesat. Hal ini disebabkan dengan banyaknya penduduk Indonesia yang mengakses internet untuk keperluan sehari-hari.

Karena begitu majunya teknologi, maka kejahatan akan dengan mudah untuk dilakukan dan mengakibatkan timbulnya masalah hukum tersendiri. Penanggulangan harus terus dilakukan dan ditingkatkan supaya pelanggaran-pelanggaran di dalam teknologi informasi tidak terus terjadi. Seperti yang terjadi saat ini, menurut penulis VPN harus diawasi oleh pemerintah.

Pornografi menjadi tren global dan mempunyai konsumen yang banyak dari berbagai dunia. Berdasarkan survei yang diadakan oleh TRU, yang bergerak dalam penelitian tentang remaja terhadap orang-orang berusia 13-26 tahun dengan 1.280 responden online yang terdiri dari 653 remaja (usia 13-19) dan 627 orang dewasa muda (usia 20-26)-antara tahun 2008 menemukan bahwa satu dari lima gadis remaja usia 13-19 tahun (22%)-dan 11% dari gadis-gadis remaja usia 13-16 tahun mengatakan mereka telah dikirim atau diposting online.[2]

Berdasarkan uraian diatas maka perlu dianalisis dan dikaji lebih lanjut mengenai permasalahan-permasalahan yang ada di kehidupan masyarakat tentang bagaimana cara kerja pemerintah dan undang-undang yang mengaturnya, dan menyusun skripsi dengan judul upaya pencegahan atas

---

[1] Widodo., 2014. Memerangi Cybercrime. Sleman: Aswaja Pressindo, h. 27

[2] Feri Sulianta., 2010. *Cyber Porn*: Bisnis atau Kriminal. Bandung: PT Gramedia, h.11

penyalahgunaan *Virtual Private Network* (VPN) oleh pengguna internet di Indonesia.

## B. Rumusan Masalah

Berdasarkan latar belakang yang telah peneliti uraikan, maka yang menjadi permasalahan dalam penelitian ini adalah:

1. Kejahatan apa yang dapat timbul akibat penyalahgunaan VPN?
2. Apa hambatan dalam menangani penyalahgunaan *Virtual Private Network* (VPN)?
3. Bagaimana upaya pencegahan untuk mengatasi penyalahgunaan *Virtual Private Network* (VPN)?

## C. Tujuan Penelitian

Adapun yang ingin dicapai dalam penelitian ini adalah untuk mendeskripsikan secara analisis tentang penangan atas penyalahgunaan *Virtual Private Network* (VPN), sedangkan secara khusus tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui kejahatan apa yang timbul akibat penyalahgunaan VPN
2. Untuk mengetahui hambatan-hambatan apa saja dalam menangani penyalahgunaan *Virtual Private Network* (VPN)
3. Untuk mengetahui upaya pencegahan atas penyalahgunaan *Virtual Private Network* (VPN)

## D. Manfaat Penelitian

1. Manfaat Secara Teoritis

Sebagai sumbangan pemikiran dalam upaya pencegahan atas penyalahgunaan *Virtual Private Network* (VPN) dengan dapat diaksesnya situs-situs terlarang oleh pengguna internet di Indonesia sesuai dengan pasal 27 UU ITE.

2. Manfaat Secara Praktis

Dapat memberi ide dan masukan untuk melakukan pengawasan terhadap *Virtual Private Network* (VPN) agar penyalahgunaan tidak terus terjadi, karena hal tersebut merupakan suatu perbuatan yang dilarang dan juga memiliki ketentuan pidana.

## II. Tinjauan Pustaka

### A. *Cyber Crime* Sebagai Bentuk Kejahatan Baru

Secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia *cyber* (*cybercrime*) adalah "upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan computer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut". [3] Menurut Freddy Haris, *cybercrime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

1. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan)
2. *Unauthorized alteration or destruction of data*
3. Mengganggu/merusak operasi *computer*
4. Mencegah/menghambat akses pada *computer*.[4]

Bentuk kejahatan lainnya seperti pornografi dalam berbagai jenis dengan mudah dapat dilihat di beberapa situs tertentu, bahkan dibeberapa *websites* dapat kita jumpai adanya *space* (ruang) untuk melakukan perjudian, misalnya dalam situs www.altavista.com disuguhi apa yang dinamakan *online gambling*, atau *online casino*, begitu pula jika masuk ke situs www.lycos.com akan ditemukan berbagai bentuk perjudian dengan nama *casino games*.[5]

### B. Pengertian *Cybercrime*

*Cyber crime* merupakan merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik itu *dial up system*, menggunakan jalur telepon ataukah *wireless system* yang menggunakan antenna khusus yang nirkabel.[6] Jika menyebut kejahatan telematika, maka yang dimaksud juga adalah *cyber crime*. *Cyber crime* tidak hanya mengunakan teknologi komputer, akan tetapi melibatkan juga teknologi komunikasi di dalam pengoperasiannya.

### C. Aturan Hukum *Cyber Crime*

Membahas aturan aturan hukum *cybercrime* memiliki tantangan tersendiri, dikarenakan hal ini aturan perundang-undangan yang mengatur tentang kejahatan siber di Indonesia masih seumur jagung. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengatur tentang kegiatan internet di Indonesia.

---

[3] Dikdik M. Arief Mansyur & Elisatris Gultom., 2005. *Cyber Law*: Aspek Hukum Teknologi Informasi. Bandung: PT Refika Aditama, h.08

[4] *Ibid*. h.09

[5] *Ibid*. h.11

[6] Abdul Wahid dan Mohammad Labib, 2005. Kejahatan Mayantara. Bandung: PT Refika Aditama, h.45

Sebelum mengonstruksi aturan-aturan hukum nasional (UU ITE) secara detail, maka menarik untuk mengkaji kembali penyusunan perangkat hukum tentang *cybercrime* yang dihasilkan oleh the G-8 dalam *communique* tanggal 9-10 Desember 1997.[7]

**D. Kejahatan *Cyber Crime* dan Bentuknya**

Kejahatan merupakan salah satu sifat fitrah manusia yang ada pada diri manusia dan terus mengalami perkembangan signifikan dengan perkembangan masyarakat itu sendiri, kejahatan yang berhubungan dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dikelompokkan dalam beberapa bentuk antara lain:

1) *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya
2) *Ilegal contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum, sebagai contoh adalah:
    a) Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain
    b) Pemuatan hal-hal yang berhubungan dengan pornografi
    c) Pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya
3) *Data forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet
4) *Cyber espionage*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran
5) *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan membuat suatu gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet

[7] Maskun,2013, Kejahatan Siber (Cyber Crime). Jakarta: KENCANA, h. 58

6) *Offence against intellectual property*, yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet
7) *Infringements of privacy*, yaitu kejahatanyang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.[8]

**E. Berlakunya Hukum Pidana Dalam Kejahatan di Dunia Maya (*Cyber Crime*)**

Dalam Pasal 1 KUHP diatur mengenai batas-batas berlakunya hukum pidana menurut waktu atau saat terjadinya perbuatan. Pasal 2 sampai Pasal 9 KUHP mengatur mengenai batas-batas berlakunya perundang-undangan hukum pidana menurut tempat terjadinya. Lebih lanjut Moeljatno mengatakan: "dasar lain yang masuk akal bahwa hukum pidana suatu negara mungkin berlaku bagi perbuatan-perbuatan yang terjadi di luar negara adalah asas melindungi kepentingan, kepentingan ini dapat dibedakan menjadi kepentingan nasional dan kepentingan internasional".[9]

**F. Prinsip Efektivitas**

Keefektifan hukum adalah situasi di mana hukum yang berlaku dapat dilaksanakan, ditaati dan berdaya guna sebagai alat kontrol sosial atau sesuai tujuan dibuatnya hukum tersebut.[10] Pembentukan UU ITE telah memberikan sumbangan yang besar bagi perkembangan dunia informasi dan transaksi elektronik. Kontrol sosial ternyata juga menjadi dasar pembentukan UU ITE, karena kemajuan yang pesat di bidang Teknologi Informasi pada saat ini telah demikian memasyarakat terutama apabila melihat penggunaan sarana komunikasi handphone.[11]

Soerjono Soekanto, menyatakan faktor-faktor yang mempengaruhi efektivitas hukum, sebagai berikut:

a. Kaidah hukum/peraturan itu sendiri
b. Petugas/penegak hukum
c. Fasilitas
d. Masyarakat dan kebudayaan
e. Prinsip pembebanan tugas kepada penegak hukum.[12]

---

[8] *Ibid*. h.51
[9] Dikdik M. Arief Mansur dan Elisatris Gultom, *op cit*.,h.41
[10] Danrianto Budhijanto, 2017. Revolusi Cyberlaw Indonesia, Bandung: PT Refika Aditama, h. 42
[11] *Ibid*.
[12] *Ibid*. h.43

## G. Penyebab Terjadinya *Cyber Crime*

Penyebab tejadinya *cybercrime* yang paling utama adalah tentang moral. Seseorang yang lemah di bidang moral luhur akan jauh dari sikap mengenal, memahami, mengendalikan dan mengatur tingkah laku yang salah dan jahat (*misconuct*), misalnya pada terseret arus untuk melancarkan kekerasan, penyerangan, membakar emosi massa dan memudahkan terjadinya kejahatan.[13]

Moralitas sekuler tidak layak untuk diikuti dan dijadikan pedoman membangun gaya hidup, karena muatan normanya mengajarkan tentang kebebasan berbuat tanpa ikatan pertanggungjawaban dengan norma keagamaan.[14] Misalnya dalam moralitas sekuler untuk mendapatkan kekayaan dan kekuasaan maka cara apapun halal untuk dilakukan, termasuk mentolelir kejahatan.

Kurangnya kontrol sosial juga menyebabkan timbulnya *cybercrime*. Pada tahun 1951, Albert J. Reiss, Jr., telah menggabungkan konsep tentang kepribadian dan sosialisasi ini dengan hasil penelitian dari aliran Chicago dan telah menghasilkan teori kontrol-sosial; teori yang di kemudian hari memperoleh perhatian serius dari sejumlah pakar kriminologi.[15] Komponen tersebut adalah: (1) kurangnya kontrol internal yang wajar selama masa anak-anak; (2) hilangnya kontrol tersebut, (3) tidak adanya norma-norma sosial atau konflik antara norma-norma dimaksud (di sekolah, orang tua, atau lingkungan dekat).[16]

Teori Bonger, memaparkan ada tujuh macam penyebab kejahatan, yaitu terlantarnya anak-anak, kesengsaraan, nafsu ingin memiliki, demoralisasi seksual, alkoholisme, rendahnya budi pekerti, dan perang.[17] Pengertian kejahatan diungkapkan oleh W.A. Bonger adalah perbuatan yang sangat anti-sosial yang memperoleh tantangan dengan sadar dari Negara berupa pemberian penderitaan (hukuman atau tindakan).[18]

---

[13] Abdul Wahid., 2002. KRIMINOLOGI & Kejahatan Kontemporer. Malang: Lembaga Penerbitan Fakultas Hukum UNISMA, h.56

[14] *Ibid.*

[15] Romli Atmasasmita., 1992. Teori dan Kapita Selekta Kriminologi. Bandung: PT Eresco, h.32

[16] *Ibid.*

[17] http://webcache.googleusercontent.com/search?q=cache:rdov_YE3uPMJ:digilib.unila.ac.id/7500/18/BAB%2520II.pdf+&cd=1&hl=id&ct=clnk&gl=id diakses pada tanggal 02 April 2019, pkl. 14.00 WIB

[18] Marwan Setiawan., 2015. Karakteristik dan Kriminalitas Anak & Remaja. Bogor: Ghalia Indonesia, h.20

## III. HASIL PENELITIAN DAN PEMBAHASAN

### A. Kejahatan Yang Timbul Dalam Penyalahgunaan *Virtual Private Network* (VPN)

Terdapat dampak untuk terjadinya kejahatan apabila seseorang melakukan penyalahgunaan *Virtual Private Network* (VPN) seperti penipuan dan pencurian data pribadi. Pencurian data pribadi apabila menggunakan *Virtual Private Network* (VPN) yang gratis atau tidak berbayar

Selain penipuan dan pencurian data persebaran video dan gambar porno bisa terjadi disebabkan oleh *Virtual Private Network* (VPN), hal ini dikarenakan *Virtual Private Network* (VPN) bisa mengakses situs yang sebelumnya sudah diblokir. Penyalahgunaan penggunaan aplikasi VPN paling sering terjadi untuk mengakses situs yang bermuatan kesusilaan.

Ketentuan pidana dalam penyalahgunaan informasi dan transaksi elektronik diatur dalam pasal 45 (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan pidana paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

### B. Hambatan Menangani Penyalahgunaan *Virtual Private Network* (VPN)

Hambatan yang sulit dilakukan dalam melakukan pencegahan adalah jaringan internet yang sangat bebas, sehingga kesulitan untuk mencari penyalahgunaan di internet. Terdapat suatu kendala dalam penyidikan *Cybercrime* antara lain:

a) Kendala yuridis, yaitu belum ada peraturan perundang-undangan yang secara khusus mengatur tentang *cybercrime*, terbatasnya pengertian alat bukti sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), dan belum adanya kewenangan penyidik untuk menggeledah sistem komputer yang diduga menjadi alat atau sasaran kejahatan

b) Kendala non yuridis, yaitu keterbatasan kemampuan dan jumlah anggota Polri yang menguasai bidang teknologi komputer, barang bukti dalam *cybercrime* mudah dihilangkan atau dihapus, adanya kesulitan mendeteksi kejahatan di bidang perbankan yang menggunakan sarana komputer; kesulitan pendeteksian kejahatan tersebut disebabkan oleh kurang tersedianya peralatan yang memadai, keengganan dari beberapa korban untuk melapor kepada Polisi, sistem keamanan dari pemilik

aset/sistem yang relatif lemah, sulit melacak keberadaan/domisili pelaku kejahatan.[19]

**C. Upaya Pencegahan Untuk mengatasi Penyalahgunaan *Virtual Private Network* (VPN)**

Berbeda dengan dinas Komunikasi dan Informatika (KOMINFO) kota Malang, Menteri Komunikasi dan Informatika (MENKOMINFO) Republik Indonesia dalam melakukan pencegahan, Menteri Komunikasi dan Informatika (MENKOMINFO) Republik Indonesia melakukan pencegahan dengan cara melakukan pemblokiran.

Pemblokiran yang di lakukan oleh Menteri Komunikasi dan Informatika (MENKOMINFO) sesuai dengan Pasal 40 (2) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berisikan bahwa pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

Dengan demikian Menteri Komunikasi dan Informatika Republik Indonesia (MENKOMINFO) berwenang melakukan pemblokiran guna melindungi kepentingan umum terhadap penyalahgunaan yang terjadi di dunia maya supaya masyarakat tidak lagi melakukan hal-hal yang melanggar hukum sesuai dengan peraturan perundang-undangan.

Pemblokiran pernah dilakukan beberapa waktu yang lalu aplikasi yang di blokir MENKOMINFO adalah aplikasi yang bernama Telegram. Aplikasi tersebut diblokir karena terdapat konten tentang terorisme, dimana hal ini terorisme merupakan hal yang dilarang di Negara Republik Indonesia, tetapi aplikasi tersebut kini sudah bisa diakses kembali.

## IV. Kesimpulan dan Saran

### A. Kesimpulan

Berdasarkan dari uraian sebelumnya dapat disimpulkan beberapa hal sebagai berikut:

1) Kejahatan dapat terjadi dikarenakan penyalahgunaan *Virtual Private Network* (VPN) seperti penipuan dan pencurian data. Hal menjadi resiko besar ketika menggunakan aplikasi VPN yang memiliki tingkat perlindungan yang rendah, seperti pada aplikasi VPN yang tidak

[19] Widodo., 2009. Sistem Pemidanaan Dalam Cyber Crime. Yogyakarta: Laksbang Meditama, h.31

berbayar. Penyebaran gambar dan video bermuatan kesusilaan bisa terjadi disebabkan penyalahgunaan *Virtual Private Network* (VPN)

2) Hambatan dalam melakukan pencegahan adalah jaringan internet yang sangat bebas, sehingga kesulitan untuk mencari penyalahgunaan di internet. Keterbatasan dan jumlah anggota POLRI yang menguasai bidang teknologi juga dan barang bukti mudah dihilangkan juga menjadi hambatan dalam melakukan pencegahan.
3) Dalam melakukan pencegahan pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan informasi yang memiliki muatan yang dilarang sesuai ketentuan peraturan perundang-undangan dan pemerintah berwenang melakukan pemutusan akses yang memiliki muatan yang melanggar hukum, hal ini sesuai dengan pasal 40 (2a) dan (2)b Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

## B. Saran

Dengan melihat kesimpulan yang telah dijelaskan sebelumnya, maka penulis ingin memberikan saran untuk ditujukan pemerintah dan masyarakat. Sebagai berikut:

**1)** Pemerintah dan instansi terkait seharusnya lebih memperhatikan dan mengawasi aplikasi *Virtual Private Network* (VPN), dikarenakan aplikasi tersebut bisa mengakses situs-situs yang dikategorikan sebagai situs yang terlarang. Dengan aplikasi *Virtual Private Network* (VPN) situs-situs yang sebelumnya sudah diblokir bisa diakses kembali, hal ini dikhawatirkan akan mempengaruhi generasi selanjutnya.

**2)** Masyarakat diharapkan untuk terus memantau apabila terdapat penyalahgunaan di internet dan melaporkan ke Dinas Komunikasi dan Informatika (KOMINFO) dan kepolisian. Untuk penggunan aplikasi *Virtual Private Network* (VPN), penulis berharap kepada masyarakat untuk lebih bijak menggunakan aplikasi VPN**.**

## Daftar Pustaka

### Buku-Buku:


Abdul Wahid., 2002. KRIMINOLOGI & Kejahatan Kontemporer. Malang: Lembaga Penerbitan Fakultas Hukum UNISMA

Abdul Wahid dan Mohammad Labib, 2005. Kejahatan Mayantara. Bandung: PT Refika Aditama

Danrianto Budhijanto, 2017. Revolusi Cyberlaw Indonesia, Bandung: PT Refika Aditama

Danrianto Budhijanto, 2017. Revolusi Cyberlaw Indonesia, Bandung: PT Refika Aditama

Feri Sulianta., 2010. *Cyber Porn*: Bisnis atau Kriminal. Bandung: PT Gramedia

Marwan Setiawan., 2015. Karakteristik dan Kriminalitas Anak & Remaja. Bogor: Ghalia Indonesia

Maskun,2013, Kejahatan Siber (Cyber Crime). Jakarta: Kencana

Romli Atmasasmita., 1992. Teori dan Kapita Selekta Kriminologi. Bandung: PT Eresco

Widodo., 2009. Sistem Pemidanaan Dalam  Cyber Crime. Yogyakarta: Laksbang Meditama

Widodo., 2014.  Memerangi Cybercrime. Sleman: Aswaja Pressindo


### Undang-Undang


Kitab Undang-Undang Hukum Pidana

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

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik