TINJAUAN YURIDIS SANKSI PIDANA PENGGUNAAN VIRTUAL PRIVATE NETWORK (VPN) YANG DIGUNAKAN UNTUK MENGAKSES KONTEN PORNOGRAFI MENURUT UNDANG-UNDANG ITE NOMOR 19 TAHUN 2016

SKRIPSI

Fery Kurniawan[1], I Dr. Afif Khalid., SHI., SH., MH, M.Kn. [2], Dr. Akhmad Munawar, SH., MH [3]

Fakultas Hukum UNISKA Muhammad Arsyad Al – Banjari Banjarmasin
Email: ferykurniawan@gmail.com

ABSTRAK

Fery Kurniawan (17810174), 2021. TINJAUAN YURIDIS PENGGUNAAN VIRTUAL PRIVATE NETWORK (VPN) YANG DIGUNAKAN UNTUK MENGAKSES KONTEN PORNOGRAFI Fakultas Hukum Universitas Islam Kalimantan Muhammad Arsyad Al Banjari Banjarmasi. Dibimbing oleh : Dr. Afif Khalid., SHI., SH., MH. dan Dr. Akhmad Munawar, SH., MH.

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui Tinjauan Yuridis Penggunaan Virtual Private Network (VPN) Yang Digunakan Untuk Mengakses Konten Pornografi. Metode penelitian yang digunakan adalah Yuridis Normatif. Unit analisis adalah Undang Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang INFORMASI DAN TRANSAKSI ELEKTRONIK Nomor 11 tahun 2008. Data yang dikumpulkan terdiri dari data primer dan data sekunder. Dengan menggunakan metode studi lInformasi dan Transaksi Elektronik ratur yang membandingkannya dengan penerapan VPN di negara lain..

Hasil penelitian menunjukkan bahwa Pengaturan hukum terhadap penggunaan Privat Virtual Network (VPN) yang digunakan untuk mengakses konten pornografi di media sosial di tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang No.11 Tahun 2008 dan UNDANG-UNDANG Pornografi saat ini masih dianggap belum urgent karena keterbatasan sarana, teknologi maupun belum adanya pihak yang merasa dirugikan sehingga permasalahan tersebut belum terekspos dan dirasa penting untuk dipecahkan adapun akibat hukum terhadap penggunaan aplikasi Virtual Private Network (VPN) untuk mengakses konten pornografi di media sosial di Tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang No.11 Tahun 2008 dan UNDANG-UNDANG Pornografi dapat dikenakan denda maupun hukuman pidana.

Kata kunci : Virtual Private Network, Pornografi

ABSTRACT

Fery Kurniawan (17810174), 2021. JURIDIC REVIEW OF THE USE OF VIRTUAL PRIVATE NETWORK (VPN) USED TO ACCESS pornography content, Faculty of Law, Islamic University of Kalimantan Muhammad Arsyad Al Banjari Banjarmasi. Supervised by : Dr. Afif Khalid., SHI., SH., MH. and Dr. Akhmad Munawar, SH., MH.

The aim of this research is to find out the Juridical Review of the Use of a Virtual Private Network (VPN) Used to Access Pornographic Content. The research method used is normative juridical. The unit of analysis is Law Number 44 of 2008 concerning Pornography and Law of Information

and Electronic Transactions Number 11 of 2008. The data collected consists of primary data and secondary data. By using the lInformation and Electronic Transaction study method, which compares it with the implementation of VPNs in other countries..
The results show that the legal regulation of the use of a Private Virtual Network (VPN) used to access pornographic content on social media is reviewed from Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 and the current Pornography Law. This is still considered not urgent because of limited facilities, technology and the absence of parties who feel aggrieved so that the problem has not been exposed and it is deemed important to solve as for the legal consequences of using a Virtual Private Network (VPN) application to access pornographic content on social media. -Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 and the Pornography LAW may be subject to fines or criminal penalties.

Keywords: *Virtual Private Network, Pornography*

PENDAHULUAN

VPN memiliki fungsi untuk memberikan keamanan privasi untuk para penggunanya didalam dunia maya. VPN merupakan hubungan antara jaringan komputer satu dengan jaringan komputer yang lain secara privat melalui jaringan internet. VPN juga dapat diartikan sebagai jaringan yang menggunakan internet sebagai media perantara antar jaringan yang bersifat privat karena hanya orang tertentu yang dapat mengakses jaringan tersebut. Pada umumnya, penggunaan VPN digunakan untuk alasan keamanan dalam bertransaksi terutama ketika mengakses suatu layanan internet dengan menggunakan Wi-Fi publik yang memungkinkan IP (Internet Protocol) yang merupakan sebuah perangkat di internet atau jaringan lokal, sehingga memungkinkan sistem dikenali oleh sistem lain yang terhubungan melalui protokol internet yang dapat dilacak oleh hackers. Selain itu, penggunaan VPN juga digunakan untuk alasan anonimitas dalam mengakses situs maupun aplikasi yang terkena penyensoran atau pemblokiran dari pemerintah di suatu negara tertentu. Sehingga hal ini yang membuat peluang munculnya kejahatan cyber dapat terjadi dengan adanya kepenggunaan VPN.

Di Indonesia pengaturan mengenai anonimitas dalam menembus pemblokiran belum diatur dengan jelas. Oleh karena itu, pemblokiran yang dilakukan oleh Pemerintah terhadap konten pornografi membuat negara Indonesia sebagai pengguna terbersar layanan VPN pada tahun 2016.

Padahal pemblokiran yang dilakukan oleh Kementerian Komunikasi dan Informatika (Kominfo) adalah sebagai upaya dari program pemerintah berupa internet positif yang berguna untuk menjadikan pengguna teknologi semakin cerdas dalam menggunakan teknologi sehingga pengaturan mengenai penggunaan Virtual Private Network belum diatur secara tegas melalui peraturan perundang-undangan di Indonesia seolah-olah pemerintah melakukan pembiaran terhadap masyarakatnya yang memperbolehkan menggunakan aplikasi VPN untuk melakukan apapun tanpa adanya batasan umur maupun kepentingan. Dampak yang akan terjadi apabila aplikasi VPN tidak diatur secara tegas didalam hukum positif indonesia maka segala bentuk pencegahan dan kebijakan yang dilakukan oleh pemerintah demi menghilangkan situs internet yang bermuatan negatif akan menjadi hal yang tidak berguna karena aplikasi. VPN masih saja dibiarkan. Berhubungan dengan dampak yang ditimbulkan apabila tidak ada regulasi dan konten pornografi maka hal yang membahayakan apabila seorang anak kecil melakukan penerobosan pemblokiran untuk melihat konten pornografi dengan aplikasi VPN. Penggunaan secara umum VPN di Indonesia dapat dipertanyakan pembatasannya ditambah lagi dengan mudahnya seseorang mengunduh aplikasi VPN didalam gadget yang membuat semua masyarakat dapat memiliki VPN dengan mudah.

METODE

1. Jenis Penelitian

Metode penelitian yang akan dilakukan dalam penyusunan skripsi ini adalah penelitian hukum yuridis normatif. Metode yuridis normatif merupakan penelitian hukum yang dilakukan terhadap asas-asas hukum dan taraf sinkronisasi hukum.[4]

[4] Soerjono Soekanto*, Pengantar Penelitian Hukum,* Jakarta: Penerbit Universitas Indonesia, 2008, hal. 51.

2. Sifat Penelitian

Sifat Penelitian ini menggunakan metode perbandingan, yang dimana penulis akan melakukan perbandingan dengan beberapa negara lain. Penelitian hukum normatif yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka. Penelitian ini dinamakan juga penelitian hukum kepustakaan.[5]

3. Sumber Bahan Hukum

a. Data primer

Penerapan sanksi VPN dinegara lain..

b. Data sekunder

Data sekunder dalam penulisan skripsi ini terdiri dari 3 (tiga) bahan hukum, antara lain bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier, yaitu sebagai berikut:

1) Bahan hukum primer, yakni bahan-bahan hukum yang mengikat, antara lain :
   a) Undang-Undang Dasar Republik Indonesia Tahun 1945
   b) Kitab Undang-undang Hukum Pidana
   c) Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi
   d) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik
   e) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggara sistem dan transaksi Internet
   f) PERMENKOMINFO Nomor 36 Tahun 2014 tentang Tata cara pendaftaran penyelenggara sistem elektronik
   g) PERMENKOMINFO Nomor 19 Tahun 2014 tentang Penanganan situs internet bermuatan negatif
   h) Surat Edaran Menkominfo Nomor 3 Tahun 2016 tentang Penyediaan layanan aplikasi dan/atau konten melalui internet

2) Bahan hukum sekunder

Bahan hukum sekunder didapat melalui studi kepustakaan dari buku maupun lInformasi dan Transaksi Elektronik ratur mengenai pandangan seorang ahli hukum.

3) Bahan hukum tersier, yaitu bahan-bahan hukum yang dapat membantu menjelaskan bahan hukum primer dan sekunder. Bahan hukum tersier dapat berupa koran, artikel, atau kamus yang memiliki hubungan dengan topik penelitian.

4. Teknik Pengumpulan Bahan Hukum

Untuk memperoleh data yang relevan digunakan inventarisasi dan pengumpulan bahan hukum dengan studi kepustakaan (*library research*). Pada studi lapangan dengan mencari dan mengumpulkan bahan-bahan bacaan yang berhubungan dengan masalah yang dibahas dalam skripsi ini seperti Peraturan Perundang-undangan, buku-buku, makalah, makalah dan hasil-hasil penelitian yang relevan.

5. Teknik Pengolahan Bahan Hukum

Setelah bahan hukum dikumpulkan, kemudian tahap selanjutnya adalah melakukan pengolahan bahan hukum, yaitu mengelola bahan sedemikian rupa sehingga bahan hukum tersebut tersusun secara runtut, sistematis, sehingga akan memudahkan penelitian melakukan analisis.

Bahan yang terkumpul melalui kegiatan pengumpulan bahan hukum memberikan makna apapun bagi tujuan penelitian. Oleh karena itu, setelah pengumpulan bahan hukum ini, peneliti kemudian melakukan kegiatan pengolahan bahan hukum.

6. Teknik Analisis Bahan Hukum

[5] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta : PT Raja Grafindo Persada, 2006, hal. 13-14.

Melakukan analisa bahan hukum merupakan kegiatan dalam penelitian yang berupa melakukan kajian atau telah terhadap hasil pengolahan bahan hukum yang dibantu dengan teori-teori yang telah didapatkan sebelumnya. Secara sederhana analisis bahan hukum ini disebut sebagai kegiatan memberikan telaah, yang dapat berarti menentang, mengkritik mendukung, menambah atau member komentar dan kemudian membuat suatu kesimpulan terhadap hasil penelitian.

HASIL DAN PEMBAHASAN

A. Pengaturan hukum terhadap penggunaan *Privat Virtual Network (VPN)* yang digunakan untuk mengakses konten pornografi di media sosial di Tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 dan UNDANG-UNDANG Pornografi

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).

1. 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* yang berkenaan dengan penggunaan *Virtual Private Network.*

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.

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

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.

Pengaturan Tindak Pidana Siber Materil di Indonesia hukum terhadap penggunaan *Privat Virtual Network* (VPN) yang digunakan untuk mengakses konten pornografi di media sosial di Tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 dan Undang-Undang Pornografi diatur dalam pidana Siber yang dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana (Undang-Undang nomor 3 Tahun 2011) maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Akan tetapi, menurut Sitompul[6] dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sama halnya seperti *Convention on Cybercrimes*, Undang-Undang Informasi Dan Transaksi Elektronik juga tidak memberikan definisi mengenai *Cybercrimes*, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrimes* tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:

Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:

a. Kesusilaan (Pasal 27 ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik);
b. Perjudian (Pasal 27 ayat (2) Undang-Undang Informasi Dan Transaksi Elektronik);
c. penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) Undang-Undang Informasi Dan Transaksi Elektronik);
d. pemerasan dan/atau pengancaman (Pasal 27 ayat (4) Undang-Undang Informasi Dan Transaksi Elektronik);
e. berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik);
f. menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) Undang-Undang Informasi Dan Transaksi Elektronik);
g. mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 Undang-Undang Informasi Dan Transaksi Elektronik);
h. dengan cara apapun melakukan akses illegal (Pasal 30 Undang-Undang Informasi Dan Transaksi Elektronik);
i. intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 Undang-Undang 19 tahun 2016);
j. Tindak pidana yang berhubungan dengan gangguan (*interferensi*), yaitu:

[6] Sitompul, Josua. 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana, PT. Tatanusa.hal.32

1) Gangguan terhadap Informasi atau Dokumen Elektronik (data *interference* - Pasal 32 Undang-Undang Informasi Dan Transaksi Elektronik);
2) Gangguan terhadap Sistem Elektronik (*system interference* –Pasal 33 Undang-Undang Informasi Dan Transaksi Elektronik);
3) Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 Undang-Undang Informasi Dan Transaksi Elektronik);
4) Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 Undang-Undang Informasi Dan Transaksi Elektronik);
5) Tindak pidana tambahan (*accessoir* Pasal 36 Undang-Undang Informasi Dan Transaksi Elektronik); dan
6) Perberatan-perberatan terhadap ancaman pidana (Pasal 52 Undang-Undang Informasi Dan Transaksi Elektronik).

Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

1) Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* - Pasal 32 Undang-Undang Informasi Dan Transaksi Elektronik);
2) Gangguan terhadap Sistem Elektronik (system *interference* –Pasal 33 Undang-Undang Informasi dan Transaksi Elektronik);
3) Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 Undang-Undang Informasi Dan Transaksi Elektronik);
4) Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 Undang-Undang Informasi Dan Transaksi Elektronik);
5) Tindak pidana tambahan (*accessoir* Pasal 36 Undang-Undang Informasi Dan Transaksi Elektronik); dan
6) Perberatan-perberatan terhadap ancaman pidana (Pasal 52 Undang-Undang Informasi Dan Transaksi Elektronik).

Adapun Pengaturan Tindak Pidana Siber Formil di Indonesia dalam Undang-Undang Informasi Dan Transaksi Elektronik mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 Undang-Undang Informasi Dan Transaksi Elektronik mengatur bahwa penyidikan terhadap tindak pidana dalam Undang-Undang Informasi Dan Transaksi Elektronik dilakukan berdasarkan ketentuan dalam Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP") dan ketentuan dalam Undang-Undang Informasi Dan Transaksi Elektronik . Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam Undang-Undang Informasi Dan Transaksi Elektronik . Kekhususan Undang-Undang Informasi Dan Transaksi Elektronik dalam penyidikan antara lain:[7]

a. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPS") Kementerian Komunikasi dan Informatika;
b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;
c. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana;
d. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketentuan penyidikan dalam Undang-Undang Informasi Dan Transaksi Elektronik dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik dan

[7] Ibid, hal.43

perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

Adapun prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut:[8]

Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian *Cybercrime* atau kepada penyidik pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam Undang-Undang Informasi Dan Transaksi Elektronik .

Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI.

Selain Undang-Undang Informasi Dan Transaksi Elektronik, peraturan yang menjadi landasan dalam penanganan kasus *cybercrime* di Indonesia ialah peraturan pelaksana Undang-Undang Informasi dan Transaksi Elektronik dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Pengaturan hukum terhadap penggunaan *Privat Virtual Network (VPN)* yang digunakan untuk mengakses konten pornografi di media sosial di tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 dan Undang-Undang Pornografi 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 namun 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 serta aturan hukum yang belum mengakomodasi permasalahan Akses pornografi menggunakan VPN karena selama ini belum ada yang merasa dirugikan sehingga permasalahan tersebut belum terekspos dan dirasa penting untuk dipecahkan.

B. Akibat hukum terhadap penggunaan aplikasi *Virtual Private Network* (VPN)

Setiap penyelenggara Sistem Elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Dalam hal ini, pemilik atau penyedia *platform* penyelenggara Sistem Elektronik bertanggung jawab terhadap penyelenggara sistem elektronik yang berkaitan dengan adanya pelanggaraan sistem elektronik. Bertanggung jawab artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggara sistem elektronik tersebut baik Penyelenggara Sistem Elektronik untuk digunakan sendiri dan untuk digunakan sebagai pelayanan publik harus menyelenggarakan Sistem Elektronik dengan andal, aman, serta beroperasi sebagaimana mestinya dan bertanggung jawab terhadap beroperasinya sistem elektronik yang dimaksud.

Penyedia *Platform* merupakan subjek hukum dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik (UU ITE) yaitu sebagai Penyelenggara Sistem Elektronik. Berdasarkan pasal 15 Undang-Undang Informasi Dan Transaksi Elektronik, penyedia *platform* sebagai Penyelenggara Sistem Elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya yakni dengan menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Ketentuan pertanggungjawaban tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa kesalahan, dan/atau kelalaian dari pihak pengguna sistem elektronik.

[8] Ibid, hal.44

Dalam Pasal 5 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik (atau yang disingkat dengan "Peraturan Pemerintah PSTE") yang menyatakan bahwa Penyelenggara Sistem Elektornik wajib memastikan sistem tidak memuat, memfasilitasi informasi yang dilarang.

Dalam Surat Edaran Menteri Kominfo Nomor 03 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet (*Over The Top*). Peraturan-peraturan tersebut mengatur secara khusus kepada pembuat dan penyedia layanan aplikasi. Dalam angka 5.4 disebutkan bahwa penyedia layanan *Over the Top* tersebut bertanggung jawab secara penuh dalam menyediakan layanan *Over the Top*.

Kewajiban penyedia layanan Over the Top berdasarkan Surat Edaran Menteri Kominfo Nomor 03 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten melalui Internet (*Over the Top*) diantaranya:[9]

1. Menaati ketentuan peraturan perundang-undangan di bidang larangan praktek monopoli dan persaingan usaha tidak sehat, perdagangan, perlindungan konsumen, hak atas kekayaan intelektual, penyiaran, perfilman, periklanan, pornografi, anti terorisme, perpajakan; dan ketentuan peraturan perundang-undangan terkait lainnya.
2. Melakukan perlindungan data sesuai dengan ketentuan peraturan perundang-undangan.
3. Melakukan filtering konten sesuai dengan ketentuan peraturan perundang-undangan;
4. Melakukan mekanisme sensor sesuai dengan ketentuan peraturan perundang-undangan;
5. Menggunakan sistem pembayaran nasional (*national payment gateway*) yang berbadan hukum Indonesia;
6. Menggunakan nomor protokol internet Indonesia;
7. Memberikan jaminan akses untuk penyadapan informasi secara sah (*lawful interception*) dan pengambilan alat bukti bagi penyidikan atau penyelidikan perkara pidana oleh instansi yang berwenang sesuai dengan ketentuan peraturan perundang-undangan; dan
8. Mencantumkan informasi dan/atau petunjuk penggunaan layanan dalam Bahasa Indonesia sesuai dengan ketentuan perundang-undangan.

Kasus pada tanggal 22 Mei 2019 pada saat Kominfo menutup akses media sosial untuk menghindari berita hoax, banyak masyarakat berbondong-bondong menggunakan VPN gratis untuk mengakses media sosial, tetapi penggunaan VPN banyak disalahgunakan seperti membuka situs yang diblokir oleh pemerintah seperti pornografi, perjudian dan lain-lain. Dari kasus tersebut, Hal yang dapat dipertanggung jawabkan oleh penyedia aplikasi adalah Penyedia aplikasi bisa melakukan filtering konten.

Filtering konten[10] nantinya akan menentukan konten apa saja yang tersedia maupun konten yang tidak boleh diakses atau diblokir tapi hal ini perlu kerja sama dengan pihak Pemerintah. Selain itu, apabila terjadi kejahatan pencurian yang diakibatkan penggunaan VPN, penyedia aplikasi dapat memberikan jaminan akses untuk penyadapan informasi secara sah (*lawful interception*) dan pengambilan alat bukti bagi penyidikan atau penyelidikan perkara pidana oleh instansi yang berwenang sesuai dengan ketentuan peraturan perundang-undangan. Hal ini sesuai dengan Pasal 33 Peraturan Pemerintah PSTE yang menyatakan bahwa untuk keperluan proses peradilan pidana, Penyelenggara Sistem Elektronik wajib memberikan Informasi Elektronik atas permintaan yang sah dari penyidik untuk tindak pidana tertentu sesuai dengan kewenangan yang diatur dalam undang-undang. Tetapi hanya pihak developer aplikasi VPN saja yang dapat melacak *IP address* pengguna jika terjadi penyalahgunaan ataupun tindakan pidana. Berkaitan dengan tanggung jawab pihak penyedia aplikasi, sesuai dengan pasal 31 Peraturan Pemerintah PSTE yang menyatakan bahwa:

"Penyelenggara Sistem Elektronik wajib melindungi penggunanya dan masyarakat luas dari kerugian yang ditimbulkan oleh Sistem Elektronik yang diselenggarakannya."

Namun mengintervensi pihak penyedia server VPN yang notabene sebagian besar berbasis di luar negeri dan belum tentu pihak penyedia peminjaman server VPN mau

[9] Surat Edaran Kominfo No. 03 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau konten melalui internet (Over the Top).

[10] Mukti Winanda dan Rizka Widyarini, "Web Content Filtering", https://keamanan-informasi.stei.itb.ac.id/2013/10/30/web-content-filtering/ diakses pada tanggal 30 maret 2021.

memberikan data seseorang yang dicari dengan cara cuma-cuma menjadi hal yang sulit. Maka dalam hal ini, langkah selanjutnya yang dapat dilakukan adalah dengan cara membeli dan mungkin akan membutuhkan biaya yang tidak sedikit karena pemeliharaan server VPN yang sangat mahal. Situasi yang lebih mengkhawatirkan lagi adalah jika penyedia jasa penyewaan server VPN adalah perusahaan yang berdomisili di negara yang sedang berkonflik dengan Indonesia maka yang akan terjadi adalah pelaku penyalahgunaan VPN akan merajalela dan merasa aman dan privasinya terlindungi.

Kementerian Komunikasi dan Informatika (Kominfo) bersama Asosiasi Penyelenggara Internet Indonesia (APJII) tengah mempertimbangkan penyusunan regulasi yang bersifat teknis terkait masalah VPN yang operasionalnya harus memiliki izin di Indonesia. Fokusnya akan diarahkan ke aplikasi VPN gratis, baik perusahaan lokal maupun Internasional. Maka dari itu penyedia aplikasi VPN harus memiliki izin dari pihak pemerintah apabila masih ingin digunakan di Indonesia, hal ini merupakan upaya yang sangat efektif bagi pemerintah dalam menyikapi VPN gratis yang ada di *Playstore* dan *appstore* yang sifatnya teknis, sehingga apabila terjadi pelanggaran, kerugian, pihak penyedia VPN dapat diberi sanksi dari Pemerintah dan ISP. Apabila ternyata Pihak penyedia Aplikasi tidak melakukan prosedur perizinan, maka pihak pemerintah dapat melakukan pemblokiran terhadap aplikasi tersebut.

Penutup

A. Kesimpulan

Berdasarkan dari uraian sebelumnya dapat disimpulkan beberapa hal sebagai berikut:

1. Pengaturan hukum terhadap penggunaan Virtual Private Network (VPN) yang digunakan untuk mengakses konten pornografi di media sosial di tinjau dari Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 dan Undang-Undang Pornografi belum di atur oleh undang-undang dinegara kita, karena modusnya adalah berbeda dengan pengaturan pornografi pada Undang-Undang Informasi Transaksi Elektronik Nomor 11 Tahun 2008 karena pelaku mengakses secara diam-diam konten yang berada pada situs yang menayangkan pornografi tanpa persetujuan pemilik situs, sehingga ada pelanggaran hak cipta.
2. Akibat hukum terhadap penggunaan aplikasi Virtual Private Network (VPN) untuk mengakses konten pornografi di Indonesia saat ini belum ada undang-undang yang mengatur mengenai sangsi yang diberikan terhadap pelaku, karena memang belum ada kasus serupa yang melaporkan karena situs pornografi di Indonesia juga dianggap Ilegal dan apalagi terlacak DEPKOMINFO maka segera di blokir sehingga pemilik situs tidak dapat menuntut kepada pengakses yang ilegal, namun hal ini berbeda dengan pengaturan diluar negeri dimana pornografi tidak ilegal, yang mengenakan pelanggaran hak cipta kepada pengguna VPN yang mengakses secara ilegal situs pornografi miliknya karena untuk konten yang bersangkutan pemilik situs membayar kepada peng upload video untuk setiap video yang di upload disitus yang bersangkutan. Selain itu selama ini belum ada kasus pencurian data yang dilaporkan karena keterbatasan perangkat oleh pemilik situs untuk mendeteksi kejahatan tersebut.

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. Diperlukan pengaturan mengenai kejahatan mengakses data tanpa izin yang mana apabila dibiarkan akan menyebabkan kerugian bagi pemilik situs yang menyediakan konten video bukan pornografi, karena pengguna dapat mengakses video tanpa harus membayar biaya menjadi member ataupun mendapat izin dari pemilik situs sehingga diperlukan suatu sistem atau teknologi yang dapat melacak penggunaan VPN pada situs yang menjadi korban pencurian data.

REFERENSI

Buku

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

Abdul Wahid., (2002). Kriminologi & Kejahatan Kontemporer. Banjarmasin: Lembaga Penerbitan Fakultas Hukum UNISMA

AgusRaharjo, (2000) Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti, Bandung, 2002.

Andi Hamzah, (1987), Pornografi Dalam Hukum Pidana: Studi Perbandingan, Jakarta: Bina Mulia

Azimah Soebagijo,(2008) Pornografi Dilarang Tapi Dicari, Jakarta : Gema Insani

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

Dikdik M. Arief Mansyur & Elisatris Gultom., (2005). Cyber Law: Aspek Hukum Teknologi Informasi. Bandung: PT Refika Aditama

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

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

Moeljatno, (2000) Asas-asas Hukum Pidana, Bina Aksara, Jakarta.

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

Sitompul, Josua. 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana, PT. Tatanusa

Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Jakarta : PT Raja Grafindo Persada, 2006

Soerjono Soekanto, Pengantar Penelitian Hukum, Jakarta: Penerbit Universitas Indonesia, 2008.

Sugiyono, Metode Penelitian Kuantitatif, Kuliatatif dan R&D, Bandung: Alfabeta, 2008

Jurnal

Carlo A.Gerungan, "Tanggungjawab Penyelenggara Sistem Informasi jika terjadi Kegagalan Sistem", Media Neliti, Vol. XXI, No. 4, 2013,https://media.neliti.com/media/publications/885-ID-tanggungjawab-penyelenggara-sistem-informasi-jika-terjadi-kegagalan-sistem.pdf

Clarke Ronald V, "Situational Crime Prevention(successfull case studies)", New York, Harrow and Haston publisher Guilderland,1997, dalam karya ilmiah Dymas Ariska Arfinanto, "Langkah Preventif Pemerintah dan Analisis Pasal 35 UU ITE terhadap Penyalahgunaan Virtual Private Network", Fakultas Hukum, Universitas Trunojoyo Madura, https://pta.trunojoyo.ac.id/ welcome/detail/140111100184 diakses pada tanggal 11 April 2021.

Helmy Prasetyo, (2013) Privasi Online dan Keamanan data,, <http://journal.unair.ac.id/download-fullpapers-palim0d249692cafull.pdf>, diakses 15 Mei 2021

Internet

http://news.okezone.com/read/2008/03/28/1/95319/pencekalan-askes-situs-porno-banyak-tantangan diakses selasa 18 Agustus Jam 12:02 WITA

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 2021, pkl. 14.00 WITA

https://kominfo.go.id/index.php/content/detail/6555/Siaran+Pers+NO.101-PIH-KOMINFO122015+Tentang+Pemblokiran+Situs+Judi+dan+Pornografi+/0/siaran_pers> diakses tanggal 21 Mei 2021

https://kbr.id/berita/052019/vpn_dilarang_di_sejumlah_negara__apa_alasannya_/99420.html , diakses pada tanggal 11 April 2021.

Mukti Winanda dan Rizka Widyarini, "Web Content Filtering", https://keamanan-informasi.stei.itb.ac.id/2013/10/30/web-content-filtering/ diakses pada tanggal 30 maret 2021.

Reska Nistanto, Situs banyak diblokir, Indonesia jadi pengguna VPN, 2016, <https://tekno.kompas.com/read/2016/03/29/08370097/Situs.Banyak.Diblokir.Indonesia.Jadi.Pengguna.VPN.Tertinggi>, [05/06/2021]

Surat Edaran Kominfo No. 03 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau konten melalui internet (Over the Top).

Teguh Arifiyadi, "Proses Pencarian Pelaku Kejahatan Transnasional melalui Interpol",https://www.hukumonline.com/klinik/detail/ulasan/lt4ffae8265d21c/kejahatan-transnasional-cybercrime-/ diakses pada tanggal 07 Agustus 2021.

Yongky Karman, "Menyoal Politik Tubuh", Tersedia (online) tersedia di www.kompas.co.id/ kompas cetak/0603/10/opini/2497595.htm diakses 20 Agustus 2021Jam 13:21 WITA

Undang-undang

Undang-Undang Dasar Republik Indonesia Tahun 1945

Kitab Undang-undang Hukum Pidana

Undang-Undang Nomor 44 Tahun 2008 Tentang Pornograf

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggara sistem dan transaksi Internet

PERMENKOMINFO Nomor 36 Tahun 2014 tentang Tata cara pendaftaran penyelenggara sistem elektronik

PERMENKOMINFO Nomor 19 Tahun 2014 tentang Penanganan situs internet bermuatan negatif

Surat Edaran Menkominfo Nomor 3 Tahun 2016 tentang Penyediaan layanan aplikasi dan/atau konten melalui internet