UNIVERSITAS KATOLIK PARAHYANGAN

FAKULTAS HUKUM

Terakreditasi Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi

Nomor : 2803/SK/BAN-PT/Ak-PPJ/S/V/2020

Tinjauan Yuridis Pertanggungjawaban Pidana Penyedia Layanan Virtual Private Network Terhadap Pelanggaran Pasal 27 Ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik

OLEH

Hansel Leo B. Siregar

NPM : 2015200119

PEMBIMBING I

Dr. Rachmani Puspitadewi, S.H., M.Hum.

PEMBIMBING II

Nefa Claudia Meliala, S.H.,M.H.

Penulisan Hukum

Disusun Sebagai Salah Satu Kelengkapan
Untuk Menyelesaikan Program Pendidikan Sarjana
Program Studi Ilmu Hukum

Tahun Sidang

2019-2020

Telah disidangkan pada Ujian

Penulisan Hukum Fakultas Hukum

Universitas Katolik Parahyangan

Pembimbing I

Dr. Rachmani Puspitadewi, S.H., M.Hum.

Pembimbing II

Nefa Claudia Meliala, S.H.,M.H.

Dekan,

Dr.iur. Liona Nanang Supriatna, S.H., M.Hum.

PERNYATAAN INTEGRITAS AKADEMIK

Dalam rangka mewujudkan nilai-nilai ideal dan standar mutu akademik yang setinggi-tingginya, maka Saya, Mahasiswa Fakultas Hukum Universitas Katolik Parahyangan yang beranda tangan di bawah ini :

Nama : Hansel Leo B. Siregar

NPM : 2015200119

Dengan ini menyatakan dengan penuh kejujuran dan dengan kesungguhan hati dan pikiran, bahwa karya ilmiah / karya penulisan hukum yang berjudul:

"Tinjauan Yuridis Pertanggungjawaban Pidana Penyedia Layanan Virtual Private Network Terhadap Pelanggaran Pasal 27 Ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik"

Adalah sungguh-sungguh merupakan karya ilmiah /Karya Penulisan Hukum yang telah saya susun dan selesaikan atas dasar upaya, kemampuan dan pengetahuan akademik Saya pribadi, dan sekurang-kurangnya tidak dibuat melalui dan atau mengandung hasil dari tindakan-tindakan yang:

a. Secara tidak jujur dan secara langsung atau tidak langsung melanggar hak-hak atas kekayaan intelektual orang lain, dan atau
b. Dari segi akademik dapat dianggap tidak jujur dan melanggar nilai-nilai integritas akademik dan itikad baik;

Seandainya di kemudian hari ternyata bahwa Saya telah menyalahi dan atau melanggar pernyataan Saya di atas, maka Saya sanggup untuk menerima akibat-akibat dan atau sanksi-sanksi sesuai dengan peraturan yang berlaku di lingkungan Universitas Katolik Parahyangan dan atau peraturan perundang-undangan yang berlaku.

Pernyataan ini Saya buat dengan penuh kesadaran dan kesukarelaan, tanpa paksaan dalam bentuk apapun juga.

Bandung, 21 Juli 2020

Mahasiswa penyusun Karya Ilmiah/ Karya Penulisan Hukum

Materai
6000

(_____)

Hansel Leo B. Siregar

2015200119

Tinjauan Yuridis Pertanggungjawaban Pidana Penyedia Layanan Virtual Private Network Terhadap Pelanggaran Pasal 27 Ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik

ABSTRAK

Proses pengolahan informasi semakin berkembang seiring dengan perkembangan teknologi. Internet merupakan salah satu kemajuan teknologi di bidang informasi yang berupa sistem komunikasi yang dapat menghubungkan jaringan antara komputer-komputer di dunia, membantu proses penyebaran dan penukaran informasi dan data antara satu sama lain dengan menghemat tenaga, waktu, biaya dan lain-lain. Namun terdapat juga berbagai macam hal yang dapat membahayakan perangkat (*device*) kita saat menggunakan internet. Dengan menggunakan *Virtual Private Network* (VPN), kita dapat mengamankan perangkat kita saat menelusuri internet, hal itu dikarenakan fungsi VPN yang mampu untuk menjaga kerahasiaan dan data-data pengguna nya.

Pemerintah Indonesia melakukan pemblokiran terhadap situs-situs yang memiliki muatan atau konten negatif, seperti situs bermuatan pornografi dan perjudian. Hal ini dilakukan guna menciptakan dan mewujudkan lingkungan dunia maya yang lebih positif. Penyedia layanan VPN cenderung memberikan layanan server dari bermacam-macam negara, hal ini lah yang sering dimanfaatkan masyarakat agar dapat mengakses situs-situs yang sudah dilakukan pemblokiran.

Kata kunci: Virtual Private Network, Situs Bermuatan Negatif, Pidana.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yesus Kristus atas segala berkat, karunia dan kebaikan-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul: Tinjauan Yuridis Pertanggungjawaban Pidana Penyedia Layanan *Virtual Private Network* Terhadap Pelanggaran Pasal 27 Ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik. Skripsi ini diajukan sebagai salah satu syarat kelulusan dan memperoleh gelar Sarjana Hukum pada Program Studi Ilmu Hukum Fakultas Hukum Universitas Katolik Parahyangan.

Pada kesempatan kali ini penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada pihak-pihak yang telah memberi bimbingan, dukungan dan bantuan selama proses penyusunan skripsi ini. Penulis mengucapkan terimakasih:

1. Kepada Tuhan Yesus Kristus karena atas karunia dan berkat-Nya, penulis selalu dikaruniai kesehatan, kemampuan dan kekuatan untuk menyusun skripsi dan menempuh pendidikan di Fakultas Hukum Universitas Katolik Parahyangan.
2. Kepada orang tua, Frans H. Siregar dan Luciana A. Narua yang tidak pernah berhenti untuk mendoakan penulis serta memberikan dukungan dalam bentuk apapun sehingga penulis dapat menempuh pendidikan di Fakultas Hukum Universitas Katolik Parahyangan.
3. Kepada adik penulis, Ramses Juan O. Siregar yang selalu memotivasi dan menemani penulis dalam menempuh pendidikan dan menyelesaikan penyusunan skripsi.
4. Kepada Ibu Dr. Rachmani Puspitadewi, S.H., M.Hum., selaku dosen pembimbing 1 yang telah bersedia meluangkan waktu di tengah kesibukan beliau untuk membimbing, mengarahkan dan membantu penulis, mulai dari penulisan proposal hingga tahap sidang penulisan hukum.
5. Kepada Ibu Nefa Claudia Meliala, S.H.,M.H., selaku dosen pembimbing 2 yang telah bersedia meluangkan waktu di tengah kesibukan beliau untuk membimbing, mengarahkan dan membantu penulis selama penyusunan skripsi hingga tahap sidang penulisan hukum.

6. Kepada Bapak Yohanes Nano Yuliono, selaku Kepala Biro Teknologi Informasi (BTI) di Universitas Katolik Parahyangan yang bersedia meluangkan waktu untuk diwawancarai penulis dan membantu penulis untuk memahami objek kajian penulis secara lebih mendalam lagi.
7. Kepada seluruh anggota JDR dan Indomie Tabrak, Deo, Shinta, Patty, Bule, Mulkam, Glen, Daniel, Boni, Tombo, William, Kelvin, Yosua, Gaodi, Devin, Inna, Meisa, Bianca, Nadhira, Bill, Sasha, Evan, Bama, Bang Lubis, Carlo, Nadya, Tae, Sakti, Ersa, Bos Jordhi, yang telah menemani dan telah menjadi teman sekaligus keluarga penulis dari awal masa perkuliahan hingga akhir masa perkuliahan.
8. Kepada seluruh senior dan junior dalam lingkup Universitas Katolik Parahyangan yang telah menjadi sosok Kakak dan Adik bagi penulis selama menempuh pendidikan dan penyelesaian skripsi ini.
9. Kepada mereka yang tidak dapat penulis sebutkan satu persatu yang turut membantu dan mendukung penulis untuk menyelesaikan pendidikan dan penyusunan penulisan hukum.

Penulis menyadari bahwa skripsi ini masih memiliki banyak kekurangan. Penulis berharap agar skripsi ini dapat bermanfaat dan berguna bagi pembaca, dan dapat memberikan wawasan bagi para pembaca.

DAFTAR ISI

Daftar Pustaka

BAB I

Pendahuluan

1.1. Latar Belakang

Proses pengolahan informasi semakin berkembang seiring dengan perkembangan teknologi. Internet merupakan salah satu kemajuan teknologi di bidang informasi yang berupa sistem komunikasi yang dapat menghubungkan jaringan antara komputer-komputer di dunia, membantu proses penyebaran dan penukaran informasi dan data antara satu sama lain dengan menghemat tenaga, waktu, biaya dan lain-lain. Perkembangan internet ini menciptakan suatu "dunia baru" yang disebut sebagai *cyberspace*. Namun kemajuan-kemajuan yang dicapai oleh manusia selalu diikuti oleh tindak pidana baru yang menyertai kemajuan tersebut. Oleh karena itu, internet ini juga memberikan dampak negatif berupa munculnya tindak pidana baru di bidang teknologi informasi dan komunikasi. Segala tindak pidana yang dilakukan dalam *cyberspace* disebut sebagai *cyber crime*, tindak pidana tersebut dapat berupa tindak pidana terhadap *confidentiality*, *integrity*, *phreaking*, *viruses*, maupun tindak pidana yang dilakukan dengan menggunakan media teknologi informasi dan komunikasi sebagai alat (seperti *cyberfraud*, *credit card fraud*, *cyberpornography*, *cyberterrorism*, dan lain-lain).[1]

Pada tanggal 23 November 2001 di Budapest, dihasilkan *Council of Europe Convention on Cybercrime* 2001 (Konvensi Dewan Eropa 2001) yang menjadi pedoman bagi negara-negara anggota *Council of Europe* maupun negara-negara bukan anggota *Council of Europe*.[2] Perbuatan yang termasuk dalam kategori tindak pidana siber diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Bab VII tentang Perbuatan yang Dilarang (Pasal 27-37). Walaupun sudah ada pengaturan mengenai *cyber crime*, pengguna internet harus tetap lebih berhati-hati dalam menjaga keamanan identitas, kode akses, informasi, maupun data penting lainnya saat menelusuri internet, terutama dalam pengolahan informasi.

[1] Sigid Suseno, Yurisdiksi Tindak Pidana Siber, (Refika Aditama : Bandung), 2012, hlm. 2
[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 diakses tanggal 10 Februari 2020PS

Pengolahan informasi sangat penting bagi perusahaan-perusahaan. Sebuah instansi baik pemerintah maupun swasta biasa menggunakan sistem *database* untuk melakukan proses pengolahan informasi satu sama lain. Sistem *database* seperti sistem jaringan skala luas atau yang disebut dengan *Wide Area Network* (WAN) ini berguna untuk menghubungkan semua kantor cabang dengan kantor pusat untuk dapat melakukan proses komunikasi data dan informasi. Salah satu alternatif untuk melakukan komunikasi data pada jaringan skala luas (WAN) adalah *Virtual Private Network* (VPN).[3] VPN merupakan satu koneksi virtual, dapat disebut seperti ini karena jaringan ini tidak memiliki bentuk secara fisik melainkan berbentuk sebagai jaringan *virtual*. Selain itu VPN merupakan suatu jaringan yang bersifat *private,* sehingga VPN mampu menghubungkan antara komputer atau *smartphone* dengan jaringan publik seperti internet secara *private*, sehingga tidak semua orang dapat terkoneksi ke dalam dan mengakses jaringan ini.[4] Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaannya. Fungsi-fungsi utama tersebut adalah sebagai berikut: [5]

1) *Confidentially* (Kerahasiaan)

   Dalam menggunakan jaringan publik tentu juga memiliki dampak negatif seperti pencurian data. VPN menggunakan sistem kerja dengan mengenkripsi semua data yang lewat melaluinya. Teknologi enkripsi ini yang menjaga kerahasiaan data ketika menggunakan VPN. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

2) *Data Integrity* (Keutuhan Data)

   Saat melakukan pertukaran data antara satu sama lain dapat memiliki gangguan saat data tersebut melewati jaringan internet yang telah melintasi berbagai negara. Berbagai gangguan tersebut dapat merusak isi

[3] Sakiwan, Kajian *Virtual Private Network* (VPN) Lapan dan Pemanfaatannya Dalam Mendukung Pengembangan E-Government. Berita Dirgantara Vol. 11 No. 4 Desember 2010: 145-152, hlm. 145
[4] Ibid hlm. 146
[5] Irawan Afrianto, Eko Budi Setiawan, Kajian *Virtual Private Network* (VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer, Majalah UNIKOM Vol.12 No. 1, hlm. 44-45

dari data, baik hilang, rusak ataupun dimanipulasi oleh orang yang tidak berwenang. VPN memiliki teknologi yang dapat mencegah hal tersebut dengan menjaga keutuhan data dimulai dari data dikirim hingga data sampai di tempat yang ditujukan.

3) *Origin Authentication* (Autentikasi Sumber)
VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya, tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain. Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil.

Karena fungsi-fungsi utama ini lah banyak perusahaan yang menggunakan VPN sebagai pilihan untuk menjaga keamanan dalam melakukan transaksi informasi satu sama lain. Solusi alternatif jaringan skala luas saat ini bisa menggunakan VPN yang lebih ekonomis dan tepat. Teknologi VPN dapat memberikan keamanan di dalam melakukan komunikasi data melalui jaringan Internet serta merupakan solusi yang efisien dan ekonomis dibandingkan dengan teknologi jaringan skala luas lainnya. Beberapa keunggulan menggunakan VPN sebagai pembanding jaringan skala luas (WAN) yang membuat banyak *telco provider* menawarkan solusi ini dan banyak perusahaan mulai beralih ke teknologi tersebut, beberapa keunggulannya adalah:[6]

1. Standarisasi, kompatibel dengan standar *protocol Internet Engineering Task Force* (IETF) dan vendor dunia lainnya

2. Lebih ekonomis, lebih murah dibandingkan dengan solusi lain karena interkoneksi dilewatkan di jaringan Internet dan tidak memerlukan perangkat khusus jika infrastruktur yang telah ada mendukung jaringan VPN.

[6] Ibid hlm. 46

3. Biaya sewa *link* yang murah dari penyedia jasa *backbone* dikarenakan menggunakan layanan jaringan baru yang lebih ekonomis seperti *MultiProtocol Labeling Switching* (MPLS).

4. Fleksibel Arsitektur, dapat dikoneksikan dengan infrastruktur yang sudah ada seperti peralatan *router*/*swtich* yang mendukung VPN.

5. Integrasi Konektifitas Multimedia yang tinggi, akses dimana saja ke global interkoneksi untuk koneksi data, suara, dan video

6. *Skalability*, memungkinkan penyedia jasa untuk tetap bisa melayani permintaan pasar tanpa harus kehilangan kesempatan.

7. *Security*, memungkinkan *traffic* kritikal bisnis dengan aman dengan digunakannya metode *tunneling* dan *enkripsi*.

8. *Managable*, sangat cocok untuk efektifitas biaya karena kemudahan dalam manajemen vendor untuk *multiple service* berbasis IP

9. *Traffic engineering*, mudah dalam pengaturan *traffic bandwidth*, mekanisme restorasi *fault* dan mekanisme proteksi

10. *Fast deployment*, cocok untuk perusahaan yang memerlukan aplikasi-aplikasi berbasis IP yang cepat perubahannya

11. Jaminan *Service Level Aggreement* (SLA) dan Jaminan Kualitas Layanan atau *Quality of Services* (QoS), jaminan layanan *uptime* bagi kebutuhan akan kestabilan interkoneksi dan jaminan yang tinggi atas koneksi dapat dipenuhi dan memungkinkan prioritas berdasarkan kritikan atau *traffic* yang sensitifitas atas *delay*.

Pemilihan produk VPN yang tepat, akan membuat jaringan dapat dihandalkan dan dapat digunakan dengan maksimal, dengan tidak menyebabkan terjadinya penurunan kinerja yang berarti. Kebijakan manajemen dan monitoring sistem jaringan juga menjadi faktor yang mempengaruhi dalam kehandalan dan keamanan sistem VPN. Dengan memilih strategi alternatif yang tepat, solusi VPN ini dapat membantu mencapai sasaran perusahaan.

Namun bukan hanya sebuah perusahaan yang dapat menggunakan fungsi dari VPN ini, umum nya setiap pengguna internet dapat menggunakan dan memanfaatkan fungsi dari VPN. Kita dapat menemukan dan mengunduh aplikasi-aplikasi yang menyediakan jasa VPN, baik secara gratis maupun tidak. Selain itu kita juga dapat mengunduh VPN sebagai *extension* dalam *Google Chrome* untuk mempermudah dan memberi keamanan saat kita menjelajahi internet, terutama ketika menggunakan Wi-Fi di tempat umum. Terdapat beberapa penyedia layanan VPN yang dapat kita temui di Internet, beragam penawaran yang diberikan seperti keamanan privasi, *server* yang lebih banyak, atau kecepatan dan kemampuan untuk menyembunyikan identitas saat menjelajahi internet. Penyedia layanan VPN pun banyak yang menyediakan layanan VPN secara gratis, dan dapat membayar apabila ingin melakukan *upgrade* atau peningkatan terhadap VPN yang digunakan. Namun penggunaan VPN yang diunduh secara gratis dapat memiliki resiko negatif yang berbahaya dan dapat merugikan pengguna VPN itu sendiri. Resiko negatif tersebut adalah:[7]

1. Pencurian Data

   Salah satu resiko negatif menggunakan VPN gratis adalah pencurian data atau penjualan data pengguna secara *illegal*. Data yang dicuri dapat meliputi identitas pengguna seperti, nama, *password*, alamat dan data penting lainnya yang kemudian akan dijual untuk kepentingan *advertisement* (iklan) pada *gadget* kita.
2. Penyebaran *Malware*

   Saat berselancar internet menggunakan VPN secara tidak langsung virus atau *malware* dapat dengan mudah masuk ke dalam perangkat kita melalui iklan-iklan yang terdapat dalam web.
3. Risiko serangan *"Man in the Middle"*

   Beberapa layanan VPN dapat berfungsi untuk melakukan serangan *Man in The Middle*[8] (MITM) dengan memanfaatkan kelemahan *Internet Protocol*, dimana penyerang berada di tengah jalur komunikasi antar pihak untuk membajak, membaca atau mencuri data bahkan menyisipkan *malware*.
4. Pengguna digunakan sebagai *Network End-Point*

---

[7] https://www.tribunnews.com/techno/2019/05/23/efek-negatif-penggunaan-vpn-yang-harus-diketahui?page=3 diakses pada tanggal 16 Agustus 2019

[8] *Man in The Middle Attack* atau MITM *attack* adalah serangan dimana pelaku yang menyerang berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Serangan *Man in The Middle* merupakan suatu tipe serangan yang memanfaatkan kelemahan *Internet Protocol.*

Pihak ketiga menggunakan alamat IP kita sebagai *Network End-Point*[9] yang digunakan untuk meningkatkan *bandwith*[10] layanan VPN untuk meningkatkan kecepatan pengguna internet lainnya. Penyedia layanan biasa nya memindahkan *bandwith* yang lebih besar untuk pengguna yang dianggap lebih menguntungkan.

5. Kebocoran alamat IP

   Kebocoran alamat IP merupakan salah satu bahaya menggunakan VPN gratis. Beberapa layanan VPN memiliki jalur rahasia yang masih memiliki celah yang dapat digunakan untuk memperbesar kemungkinan pencurian dan kebocoran alamat IP.

Namun, VPN tidak hanya memberikan kerugian bagi pengguna nya saja. VPN juga memberikan kerugian bagi usaha pemerintah dalam menciptakan internet sehat. Kita dapat melihat tujuan dari Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 19 Tahun 2014 Tentang Penanganan Situs Internet Bermuatan Negatif (Permen Penanganan Situs Negatif) pada Pasal 2 yang mengakatan bahwa:

> *"Tujuan Peraturan Menteri ini, yaitu:*
>
> *a.memberikan dasar bagi Pemerintah dan masyarakat terhadap pemahaman situs internet bermuatan negatif dan peran bersama dalam penanganannya; dan b.melindungi kepentingan umum dari konten internet yang berpotensi memberikan dampak negatif dan atau merugikan."*

Dalam penelitian yang dibuat oleh Adian Fatchur Rochim dan Andrian Satria Martiyanto mengatakan bahwa Sistem VPN adalah suatu cara untuk membuat sebuah jaringan yang bersifat *private* dan aman dengan memanfaatkan jaringan publik seperti internet. Data dalam jaringan tersebut tidak dapat diketahui oleh pengguna lain di jaringan publik karena data tersebut dilewatkan pada *tunnel* (jalur) yang dibentuk oleh VPN.[11] Dengan menggunakan VPN, alamat IP[12] (*IP Address*) para pengguna akan diganti secara otomatis

---

[9] Perangkat atau alat yang terhubung ke LAN atau WAN dan menerima komunikasi bolak-balik di seluruh jaringan.

[10] *Bandwidth* (lebarpita) dalam ilmu komputer adalah suatu penghitungan konsumsi data yang tersedia pada suatu telekomunikasi. Dihitung dalam satuan *bits per seconds* (bit per detik). Perhatikan bahwa *bandwidth* yang tertera komunikasi nirkabel, modem transmisi data, komunikasi *digital*, elektronik, dll, adalah *bandwidth* yang mengacu pada sinyal analog yang diukur dalam satuan *hertz* (makna asli dari istilah tersebut) yang lebih tepat ditulis *bitrate* daripada *bits per second*.

[11] Adian Fatchur Rochim dan Andrian Satria Martiyanto, Desain dan Implementasi Web Proxy dan VPN Akses (Studi Kasus Undip), *Jurnal Sistem Komputer – Vol. 1 No.1 Tahun 2011, ISSN: 2087-4685,* hlm. 31

[12] IP *Address* (*internet protocol address*) merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan internet. Angka 32 bit digunakan untuk

dengan alamat IP yang disediakan oleh penyedia layanan VPN. Oleh karena itu, melalui penggunaan VPN seseorang dapat mengakses ke berbagai situs-situs yang memiliki muatan negatif, seperti situs-situs yang memiliki muatan pornografi, melanggar kesusilaan, memiliki muatan perjudian atau situs-situs muatan negatif lainnya. Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 Tentang Penanganan Situs Internet Bermuatan Negatif Pasal 4:

> *"(1) Jenis situs internet bermuatan negatif yang ditangani sebagaimana dimaksud dalam Pasal 3 hurufa, yaitu:*
>
> *a. pornografi; dan*
>
> *b. kegiatan ilegal lainnya berdasarkan ketentuan peraturan perundang-undangan.*
>
> *(2) Kegiatan ilegal lainnya sebagaimana dimaksud pada ayat (1) huruf b merupakan kegiatan ilegal yang pelaporannya berasal dari Kementerian atau Lembaga Pemerintah yang berwenang sesuai ketentuan peraturan perundang-undangan."*

Masyarakat dapat membantu Menteri Komunikasi dan Informatika (KOMINFO) dalam hal pemblokiran ini dengan memberikan aduan terhadap situs-situs yang memiliki muatan negatif kepada pihak KOMINFO. Berdasarkan data statistik, jumlah aduan paling banyak adalah situs-situs yang memiliki muatan pornografi dan perjudian. Jumlah aduan terhadap situs pornografi berjumlah 1.038.798 aduan, sedangkan untuk situs bermuatan perjudian sejumlah 199.489 aduan.[13]

Situs-situs bermuatan negatif tersebut seharusnya tidak bisa diakses oleh masyarakat di Indonesia karena situs-situs tersebut sudah diblokir oleh pemerintah, namun dengan menggunakan alamat IP (alamat IP di luar wilayah Indonesia) yang disediakan oleh penyedia layanan VPN maka situs-situs tersebut menjadi bisa diakses.

---

alamat IP *Address* versi IPv4 dan angka 128 bit digunakan untuk IP Address versi IPv6 untuk menunjukkan alamat dari komputer pada jaringan internet berbasis TCP/IP. (http://technopark.surakarta.go.id/id/media-publik/komputer-teknologi-informasi/191-ip-address-fungsi-dan-kelas-ip diakses tanggal 21 April 2020 pukul 11.12)

[13] https://www.kominfo.go.id/statistik diakses tanggal 20 Juni 2020 pukul 22.16

VPN dapat dikatakan menjadi celah terhadap pemblokiran situs-situs bermuatan negatif. Usaha pemerintah untuk menjaga kepentingan umum dalam lalu-lintas internet menjadi tidak efektif karena penyalahgunaan VPN yang dilakukan oleh masyarakat. Pengetahuan dan pemahaman masyarakat terhadap penggunaan teknologi informasi dan komunikasi terus meningkat, namun tetap menyalahgunakan fungsi dari internet sehingga dapat memberikan dampak buruk bagi perkembangan dunia maya (*cyber space*). Penggunaan VPN secara negatif ini juga memberikan dampak buruk bagi pertumbuhan dan perkembangan bagi golongan masyarakat yang masih di bawah umur.

Banyak negara yang sudah memiliki pengaturan terhadap penggunaan VPN ini, salah satu contohnya adalah Cina. Menurut penulisan Keijing Yang pada tahun 2017, terdapat dua alasan mengapa Cina memiliki aturan ketat terhadap penggunaan VPN, yaitu kemampuan teknologi yang dapat dipersalahgunakan dan adanya alasan politik-ekonomi. Cina telah berulang kali mengumumkan peraturan tentang penggunaan VPN dan memperbarui peraturan ini secara teratur untuk membuat peraturan lebih ketat dan lebih teknis. Bahkan pada empat bulan pertama tahun 2017, peraturannya telah diperbarui sekali lagi. Semua pengguna VPN harus mendapatkan lisensi untuk menggunakannya, dan lisensi tersebut tidak dapat diperdagangkan di antara perusahaan atau perorangan.[14]

Untuk di Indonesia sendiri, belum ada aturan-aturan hukum yang mengatur secara spesifik terhadap penyedia layanan maupun penggunaan VPN ini. Indonesia sudah memiliki 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 (UU Perubahan Atas UU ITE) sebagai regulasi yang mengatur kejahatan di dunia maya (*cybercrime*). Apabila kita melihat Pasal 27 ayat (1) dan ayat (2) dari UU ITE yang berbunyi:

> *"(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.*

[14] Keijing Yang, The Door Is Closed, But Not Locked: China's VPN Policy (Washington, D.C.: 2017) hlm. 6

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian."

Kita dapat melihat bahwa penyedia layanan aplikasi VPN memenuhi syarat pelanggaran dari ketentuan Pasal 27 ayat (1) dan ayat (2) ini, karena VPN sebagai salah satu aplikasi yang membuat dapat diaksesnya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan dan memiliki muatan perjudian. Sebagaimana yang dimaksud dalam Pasal 4 ayat (1) Permen Penanganan Situs Negatif bahwa pelanggaran kesusilaan dan perjudian termasuk dalam situs yang memiliki muatan negatif. Walaupun memang pengguna VPN lah yang menyalahgunakan dari fungsi VPN tersebut, namun penyedia layanan VPN lah yang menyediakan fasilitas tersebut.

Fakta-fakta di atas melatarbelakangi penulis dalam melakukan penelitian ini, karena regulasi mengenai penggunaan dan bagi penyedia layanan suatu aplikasi masih dianggap belum lengkap. Pertanggungjawaban pidana dan perlindungan hukum terhadap penyedia layanan VPN menjadi fokus utama penulis dalam melakukan penelitian yang berjudul:

Tinjauan Yuridis Pertanggungjawaban Pidana Penyedia Layanan *Virtual Private Network* Terhadap Pelanggaran Pasal 27 Ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Mengenai Informasi dan Transaksi Elektronik

1.2. Rumusan Masalah

Dari uraian latar belakang di atas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Apakah penyedia layanan VPN dapat dijerat atau diminta pertanggungjawaban pidana berdasarkan pasal 27 ayat (1) dan (2) UU ITE?
2. Bagaimana perlindungan hukum terhadap penyedia layanan *Virtual Private Network?*

1.3. Tujuan Penelitian dan Manfaat Penelitian

Berdasarkan rumusan masalah di atas, maka penulisan ini bertujuan untuk:

1. Untuk apakah penyedia layanan VPN dapat dijerat atau diminta pertanggungjawaban pidana berdasarkan pasal 27 ayat (1) dan (2) UU ITE.
2. Untuk mengetahui bentuk perlindungan hukum terhadap penyedia layanan *Virtual Private Network*.

Penelitian ini memiliki manfaat teoritis dan manfaat praktis yaitu, sebagai berikut:

1. Manfaat teoritis, yaitu untuk memberikan pemahaman mengenai pertanggungjawaban pidana penyedia layanan *Virtual Private Network* serta pengetahuan mengenai perlindungan hukum penyedia layanan *Virtual Private Network*.
2. Manfaat praktis, yaitu penelitian ini diharapkan dapat membantu memberikan kepastian hukum terhadap penyedia layanan *Virtual Private Network*, serta dapat membantu untuk menjaga perkembangan dunia maya (*cyber space*) yang positif dan sehat.

1.4. Metode Penelitian

1.4.1. Sifat Penelitian

Penelitian ini bersifat deskriptif analitis. Deskriptif analitis adalah metode yang memberikan gambaran secara obyektif mengenai sesuatu yang sedang diteliti melalui data yang sudah terkumpul, kemudian hasil tersebut diolah dan dianalisis untuk mendapatkan suatu kesimpulan.[15] Dalam penelitian ini akan dijelaskan lebih jauh mengenai VPN dan dikaitkan dengan teori-teori hukum pidana dan peraturan-peraturan yang berlaku di Indonesia. Setelah dijelaskan lebih lanjut mengenai pokok penelitian di atas, kemudian akan dianalisis dan disimpulkan bagaimana hukum positif di Indonesia mengatur pertanggungjawaban pidana penyedia layanan VPN.

1.4.2. Metode Pendekatan

Penelitian ini menggunakan metode pendekatan yuridis normatif. Menurut Soerjono Soekanto pendekatan yuridis normatif yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan

[15] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, (Alfabeta:Bandung, 2009) hlm.135

cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.[16] Penelitian yang akan dibuat oleh penulis akan dilakukan dengan meneliti bahan pustaka atau data sekunder yang berkaitan dengan topik pembahasan penelitian ini, yaitu mengenai beberapa undang-undang yang mengatur tentang informasi teknologi, *cyber crime* dan kriminalisasi tindak pidana, juga mengkaji teori-teori yang berkaitan dengan pembahasan dalam penelitian ini. Metode ini digunakan agar dapat memberikan jawab dan agar dapat menarik kesimpulan terhadap masalah hukum yang terdapat dalam penelitian ini.

1.4.3. Sumber Data

Penelitian ini akan menggunakan sumber data sekunder. Data sekunder yaitu data yang telah dikumpulkan untuk maksud selain menyelesaikan masalah yang sedang dihadapi. Dalam penelitian ini yang menjadi sumber data sekunder adalah literatur, artikel, jurnal serta situs di internet yang berkenaan dengan penelitian yang dilakukan.[17]

Sumber data yang digunakan dalam penelitian ini antara lain:

a. Bahan hukum primer antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 19 Tahun 2014 Tentang Penanganan Situs Internet Bermuatan Negatif, Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Peraturan Mahkamah Agung Republik Indonesia Nomor 13 Tahun 2016 Tentang Tata Cara Penanganan Perkara Tindak Pidana Oleh Korporasi (Perma Korporasi).

b. Bahan hukum sekunder yaitu bahan yang memberi penjelasan mengenai bahan hukum primer antara lain: buku, jurnal, karya tulis ilmiah, doktrin dan wawancara yang dapat memberikan penjelasan mengenai topik dalam penelitian ini.

[16] Soerjono Soekanto & Sri Mamudji, Penelitian Hukum Normatif (Suatu Tinjauan Singkat), (Jakarta: Rajawali Pers, 2001), hlm. 13-14
[17] Sugiyono, Metode Penelitian Kuantitatif Kualitatif dan R&D Cet. Ke 8, (Bandung: Alfabeta, 2009), hlm. 137

c. Bahan hukum tersier berupa: Kamus Besar Bahasa Indonesia dan Kamus Hukum, serta bahan lainnya yang dapat memberikan penjelasan mengenai topik dalam penelitian ini.

1.5. Sistematika Penulisan

BAB I : Pendahuluan

Dalam bab ini akan berisi pendahuluan uraian latar belakang masalah yang akan dibahas dalam penelitian ini. Kemudian berdasarkan uraian latar belakang masalah tersebut, didapatkan identifikasi atau rumusan masalah, tujuan penelitian, serta kegunaan penelitian. Selain itu bab ini akan menjelaskan metode penelitian serta sistematika penulisan dari penelitian ini

BAB II : Penjelasan Mengenai *Virtual Private Network* dan Regulasi nya di Indonesia

Dalam bab ini akan dijelaskan pengertian lebih lanjut mengenai *virtual private network*, dan regulasi-regulasi yang terkait dengan *virtual private network* di Indonesia.

BAB III : Teori-teori Hukum Pidana yang Berkaitan dengan Penyedia Layanan *Virtual Private Network*

Dalam bab ini akan dijelaskan lebih lanjut tentang teori-teori hukum pidana yang berlaku sebagai perlindungan hukum terhadap penyedia layanan *virtual private network*.

BAB IV: Analisis Terhadap Pertanggungjawaban Pidana Penyedia Layanan *Virtual Private Network* Berdasarkan UU ITE

Dalam bab ini akan menganalisis fakta-fakta yang ditemukan mengenai penulisan hukum ini guna menjawab pertanyaan yuridis dalam rumusan masalah.

BAB V : Kesimpulan dan Saran

Dalam bab ini akan ditarik suatu kesimpulan atas penelitian yang dilakukan melalui pembahasan dalam bab-bab sebelumnya dan saran yang relevan dengan hasil penelitian.