Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

PENGGUNAAN APLIKASI *VIRTUAL PRIVATE NETWORK* (VPN) *POINT TO POINT TUNNELING PROTOCOL* (PPTP) DALAM MENGAKSES SITUS TERBLOKIR

Marisa Dika Andini
Fakultas Hukum Universitas Padjadjaran
Marisa.dikasuwandi@gmail.com

Muhamad Amirulloh
Fakultas Hukum Universitas Padjadjaran
muhamad.amirulloh@unpad.ac.id

Helitha Novianty Muchtar
Fakultas Hukum Universitas Padjadjaran
Helitha.novianty@unpad.ac.id

Abstract

The discovery of a Virtual Private Network (VPN) makes it easy to access the internet wherever and whenever. Many service providers see the advantages of VPN being commercially usable, VPNs are very vulnerable to hacker attacks, cracking that supports data or information from VPN application users, this research offers to provide information about VPN security Point to Point Tunneling protocol (PPTP) and whether the VPN security system has been licensed and is in accordance with applicable law or not. This research is normative juridical. By using analytical descriptive analysis, this research provides facts about VPN security point to point tunneling protocol (PPTP) in accessing blocked sites, discussed with the Electronic Transaction Information Act.

Keywords: *Virtual Private Network* (VPN), *point to point tunneling protocol* (PPTP), *Blocked Site,*

Abstrak

Penemuan *Virtual Private Network* (VPN) memberi kemudahan untuk mengakses internet dimanapun dan kapanpun. Banyak penyedia layanan melihat keuntungan bahwa VPN ini bisa digunakan gratis secara komersial, VPN sangat rentan dari serangan *hacker, cracking* yang mampu mencuri data atau informasi dari pengguna aplikasi VPN, penelitian ini bertujuan untuk memberikan informasi mengenai keamanan VPN *Point to Point Tunneling protocol* (PPTP) dan apakah sistem keamanan VPN tersebut sudah mendapatkan perizinan dan sesuai dengan Undang-Undang yang berlaku atau tidak. Penelitian ini bersifat yuridis normatif. Dengan menggunakan pendekatan deskriptif analitis, Penelitian ini memberikan fakta-fakta mengenai keamanan VPN *point to point tunneling protocol* (PPTP) dalam mengakses situs terblokir, dikaitkan dengan Undang-undang Informasi Transaksi Elektronik.

Kata kunci: *Virtual Private Network* (VPN), *point to point tunneling protocol* (PPTP), Situs Terblokir.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

PENDAHULUAN

Perkembangan Teknologi Informasi kini sangat cepat dan signifikan, jauh berbeda dengan masa awal kehadirannya. Era globalisasi telah menempatkan peranan teknologi informasi ke dalam suatu posisi yang sangat strategis karena dapat menghadirkan suatu dunia tanpa batas, jarak, ruang dan waktu serta dapat meningkatkan produktivitas serta efisiensi. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi dan kerangka hukum yang berlangsung secara cepat dan signifikan. Secara pesat, teknologi ini mengubah cara hidup masyarakat, di mana batas ruang dan waktu sudah tidak menjadi kendala besar (*borderless)*. Bahkan kehadiran internet yang sangat fenomenal ini semakin mengukuhkan pendapat bahwa teknologi informasi dan komunikasi telah menjadi *mainstream* budaya masyarakat dunia saat ini.[1]

Indonesia adalah salah satu negara Asia Tenggara yang banyak mengakses internet. Berdasarkan hasil studi polling Indonesia yang bekerja sama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dari total populasi sebanyak 264 juta jiwa penduduk Indonesia, ada sebanyak 171, 17 juta jiwa atau sekitar 64,8 persen yang sudah terhubung ke internet. Angka ini meningkat dari tahun 2017 sebanyak 54, 87 persen. Dari survei APJII bahwa pengguna internet di Indonesia dari tahun ke tahun terus meningkat.[2] Hal ini menjadi kebutuhan masyarakat yang tidak bisa lepas dari penggunaan internet. Sebelumnya, di tahun 1996 seorang karyawan *Microsoft* bernama Gurdeep Singh Pall menemukan server *Virtual Private Network* (atau disingkat dengan VPN) yang memungkinkan penggunanya mendapatkan koneksi internet yang aman ke kantor sehingga efektif apabila pekerja dapat mengerjakan tugas kantornya di rumah, server itu bernama PPTP (*Point to Point Tunneling Protocol*). VPN dibangun hanya untuk kepentingan perusahaan besar, militer dan bukan untuk penggunaan komersial. Tujuan penggunaan VPN ini tadinya hanya diperuntukkan Perusahaan untuk menghubungkan kantor-kantor yang terpisah secara geografis dengan menggunakan jaringan privat terenkripsi yang bisa melindungi informasi rahasia Perusahaan.[3]

Menurut IETF*, Internet Engineering Task Force, VPN is an emulation of a private Wide Area Network (WAN) using shared or public IP facilities, such as the*

[1] Muhammad Amirulloh, "*Hukum Teknologi Informasi dan Komunikasi (TIK) sebagai Hukum Positif di Indonesia dalam Perkembangan Masyarakat Global",* Bandung: Unpad Press, 2016, hlm 4.

[2]Yudha Pratomo,"APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa", https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa , diakses pada tanggal 04 September 2019.

[3] Alfons Tanujaya, "Apa itu VPN dan Mengapa VPN membuat Koneksi Internet jadi Aman",https://infokomputer.grid.id/read/12313003/apa-itu-vpn-dan-mengapa-vpn-membuat-koneksi-internet-jadi-aman diakses pada tanggal 16 Juni 2019.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

internet or private IP backbones.[4] Dengan kata lain, VPN sebagai alat untuk mengubah IP address, rute lalu lintas dan menyambungkan dengan server yang aman disebuah lokasi yang berbeda, sehingga membuat komputer maupun smartphone seseorang berada di lokasi tersebut.

Ada beberapa jenis VPN dan yang paling umum dan sering ditemui adalah VPN PPTP *(Point to Point tunneling Protocol).* PPTP merupakan protokol jaringan yang dikembangkan oleh *Microsoft* dan *Cisco* yang memungkinkan pengamanan transfer data dari *remoteclient* ke *server* pribadi instansi dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan yang terdapat pada PPTP adalah pengembangan dari *remote access Point to Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP membungkus paket PPP menjadi IP *datagrams* agar dapat ditransmisikan melalui internet atau jaringan publik berbasis TCP/IP. PPTP juga dapat digunakan pada jaringan *privateLAN-to-LAN.*[5]

Meskipun Pembuatan VPN ini digunakan hanya untuk Perusahaan, banyak penyedia layanan melihat keuntungan bahwa VPN ini bisa digunakan oleh komersial atau perorangan dengan banyaknya *Wi-fi Hotspot* dan bahkan memberikan layanan internet secara gratis. Maka dari itu perlu dibutuhkan enkripsi yang aman untuk melindungi data penting yang dikirimkan melalui jaringan nirkabel, seperti dalam melakukan internet banking yang harus memasukkan kata sandi, informasi data pribadi, dan pada saat melakukan belanja online.

Penggunaan VPN secara komersial tidak menutup kemungkinan pihak atau masyarakat melakukan kegiatan hal yang positif namun pula dapat bersifat secara negatif. Karena itu banyak kejahatan yang merajalela dan mengakibatkan timbulnya masalah hukum tersendiri. Diantaranya Mengakses situs terblokir menjadi hal yang sudah lama dikonsumsi oleh berbagai dunia yang kegiatan aksesnya berkaitan dengan unsur Pornografi, Hoax, dan lainnya. Internet merupakan alat yang paling efektif untuk menyebarkan materi pornografi, berita hoax, terorisme, bisnis prostitusi, dan kejahatan lainnya dibandingkan dengan media komunikasi lainnya. Internet memiliki kemampuan untuk mengkonvergensikan segala bentuk media cetak, penyiaran, film, atau telekomunikasi dalam sebuah media yang disebut *Global Network*. Keistimewaan yang dimiliki internet tersebut menjadikan internet sebagai media komunikasi yang paling sempurna saat ini untuk menyebarkan berbagai macam informasi, termasuk pula yang mengandung unsur berita hoax.[6]

---

[4] Direktorat Sistem & Teknologi Informasi ITB, "Layanan VPN ITB", https://ditsti.itb.ac.id/layanan-vpn/ , diakses pada tanggal 16 Juni 2019.

[5] *Ibid.*, hlm 188.

[6] Andi Hamzah dan Niniek Suparni, *"Pornografi dan Pornoaksi dalam hukum pidana: suatu studi perbandingan*", Jakarta: Penerbit Universitas Trisakti, 2010, hlm 90.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Salah satu penyebab utama meningkatnya aktivitas *Cybercrime* adalah karena mudahnya seseorang untuk mengakses situs-situs tersebut melalui internet baik itu sedang berada dirumah, toilet, restoran, sekolah, dan lain-lain ditambah lagi dengan penggunaan VPN yang memungkinan bagi setiap orang untuk mengakses internet tanpa diawasi oleh Pemerintah. Kasus yang besar terjadi baru-baru ini 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 kabar yang tidak mengenakan terjadi akibat menggunakan VPN yaitu terjadi pencurian yang mengakibatkan uang di rekening korban tersebut menghilang akibat menggunakan VPN yang gratis. Kebanyakan Aplikasi VPN yang terdaftar di Playstore tidak memiliki izin atau gratis sehingga kerahasiaan pengguna tidak terjaga karena VPN gratis hanya mengutamakan kecepatan dalam berselancar internet. Selain itu karena kebutuhan media sosial dalam keadaan mendesak masyarakat pada saat itu tidak memikirkan data yang ada pada telepon genggam miliknya. Menurut *Country Director Palo Alto Networks* Indonesia Surung Sinamo, Penggunaan VPN tidaklah menjadi masalah jika hanya membuka media sosial saja, tetapi VPN bisa mengancam keamanan data pengguna jika digunakan untuk mengakses Platform yang menyimpan data-data bernilai tinggi seperti layanan perbankan, teknologi financial *(fintech),* akses digital, dan lainnya.[7]

Kementerian Komunikasi dan Informatika sedang mengkaji kemungkinan untuk mengatur izin untuk VPN yang bersifat teknis setelah layanan tersebut jamak digunakan saat pembatasan akses media sosial pada tanggal 22 Mei 2019 lalu. Maka dari itu dengan banyaknya penyalahgunaan *Virtual Private Network* perlu dipertanyakan bagaimana keamanan dan keandalan VPN untuk menjaga lalu lintas internet seseorang baik itu di Indonesia maupun di Negara lain. Selain itu bagaimana dengan pengaturan izin yang ada di Indonesia terkait penggunaan Aplikasi *Virtual Private Network (VPN).* Berkaitan dengan kasus, pada tanggal 12 Juni 2019, KOMINFO (Kementerian Komunikasi dan Informatika) sedang mempertimbangkan penyusunan regulasi yang bersifat teknis terkait VPN yang harus memiliki izin di Indonesia. Hal ini diperlukan untuk diatur agar data pribadi dapat terlindungi, regulasi ini terfokus pada VPN gratis baik lokal maupun internasional.[8]

---

[7] Cindy Mutia Annur, Ramai Dicari Usai Kerusuhan 22 Mei, ini Sisi Bahaya dari Pemakaian VPN, https://katadata.co.id/berita/2019/05/23/ramai-dicari-usai-kerusuhan-22-mei-ini-sisi-bahaya-dari-pemakaian-vpn , diakses pada tanggal 04 September 2019.

[8]Aditya Pandji, "Kominfo Mau bikin Aturan dan izin Khusus Aplikasi VPN, https://kumparan.com/@kumparantech/kominfo-mau-bikin-aturan-dan-izin-khusus-aplikasi-vpn-1rGIlEWcY8f diakses pada tanggal 16 Juni 2019.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

METODE PENELITIAN

Metode pendekatan yang digunakan pada penelitian ini adalah yuridis normative. Dengan metode ini data diperoleh dari studi kepustakaan *(library research)* dan studi peraturan perundang-undangan yang berkaitan dengan objek pembahasan penelitian ini. Pendekatan metode yuridis normative adalah penulisan kepustakaan yang didominasi dengan menggunakan data-data sekunder, baik yang berupa bahan hukum primer seperti kumpulan peraturan-peraturan, bahan hukum sekunder seperti hasil karya ilmiah para sarjana hukum, maupun bahan hukum tersier yang meliputi bahan-bahan bersumber dari internet. Metode analisis data yang digunakan pada penelitian ini dilakukan secara yuridis normative kualitatif, yaitu dengan mengkaji serta menganalisis data berdasarkan asppek hukum dan tanpa menggunakan diagram-diagram atau data statistik.

HASIL DAN PEMBAHASAN

Keamanan dan Keandalan VPN dalam mengakses situs terblokir berdasarkan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Tujuan dari penggunaan aplikasi VPN ialah untuk mengamankan data pada suatu jaringan yang bersifat *private* dan aman menggunakan jaringan publik atau internet sehingga penggunaan aplikasi VPN memberikan keamanan data bagi penggunanya. Dalam Pasal 15 UU ITE menyatakan bahwa setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik. Namun sisi gelap dari penggunaan aplikasi VPN ini ialah dapat di akses konten-konten yang terlarang seperti pornografi, perjudian, konten kekerasan dan masih banyak lagi konten berbahaya lainya.

Hal itu biasa saja karena hampir sekitar 3 juta aplikasi yang ada di *playstore* maupun *appstore* dapat diakses secara bebas oleh siapa saja. VPN di Indonesia seolah-olah dibiarkan bahkan dilegalkan, karena jika kita telusuri bersama di google *playstore* banyak sekali aplikasi VPN gratis maupun berbayar. Maka dari itu menjadi percuma tindakan pemerintah memblokir beberapa situs yang dianggap terlarang tapi masyarakat Indonesia masih bisa mengakses situs tersebut. Hal ini tentu bertentangan dengan tujuan pemblokiran menurut Peraturan Menteri Komunikasi dan Informatika No. 19 tahun 2014 tentang Penanganan Situs Internet bermuatan Negatif Pasal 2 huruf b yang berbunyi :

> “Penyaringan Konten negatif bertujuan untuk melindungi kepentingan umum dari konten internet yang berpotensi memberikan dampak negatif atau merugikan".

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Dapat diaksesnya situs-situs yang diblokir tentu bagi masyarakat akan timbul inspirasi melakukan kejahatan seperti pemerkosaan, terorisme, dan apabila dibiarkan negara Indonesia perlahan-lahan akan hancur dikarenakan kejahatan didunia maya. Salah satu kegunaan VPN yang negatif lainnya adalah melakukan kejahatan *cybercrime* seperti *hacking, cracking,* dan lain sebagainya. Dengan menggunakan teknologi *anonym* alias terlindunginya identitas si pelaku, maka sangat berbahaya bila penggunaan VPN disalahgunakan oleh oknum-oknum yang tidak bertanggung jawab.

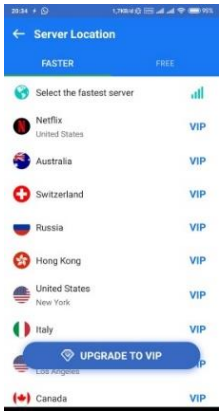
> *"Blocking by the government can still be opened using a VPN application. Indonesia is the largest VPN user in the world due to the number of websites blocked by the government. VPN creates a new identity that can be used to create a new identity and can be used to break the internet block in a country. In a survey made by the Global Web Index, 41 percent of internet users in Indonesia use VPNs to access sites on the internet. Content accessed using VPNs such as iTunes, Netflix, Youtube, Vimeo and negative content sites such as pornography".*[9]

Pada tahun 2018, negara dengan penggunaan VPN terbesar di dunia adalah Indonesia dan India sebanyak 38 persen menggunakan VPN. Persentase ini lebih tinggi dari rata-rata regional. Di Asia Pasifik hanya 30 persen populasi pengakses internet menggunakan VPN. Sedangkan Di Eropa, hanya 17 persen populasi pengakses internet menggunakan VPN.[10] Di toko aplikasi *Playstore*, banyak VPN ditawarkan oleh penyedia aplikasi lebih dari 50 juta perangkat misalnya Turbo VPN, Hola VPN, dan VPN Hub. VPN Hub, yang terkait dengan Pornhub, telah dipasang pada lebih dari 5 (Lima) juta perangkat. Salah satunya adalah miniVPN yang dibuat oleh miniVPN team. MiniVPN ini tidak menggunakan konfigurasi apapun sehingga pengguna dapat berselancar di internet dengan menggunakan teknologi anonym.

[9] Wahyu Nugroho, dkk, "The Prevention of Negative Content by using VPN (Virtual Private Network) towards website that is blocked by the government", *Indonesia Journal of Criminal Law Studies*, Universitas Negeri Semarang, 4(2) (2019), 106-116.

[10] Ahmad Zaenudin, "*Ramai-ramai Menggunakan VPN, tapi Amankah*?" https://tirto.id/ramai-ramai-menggunakan-vpn-tapi-amankah-dYLs , diakses pada tanggal 04 April 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166



Gambar: https://play.google.com/store/apps/details?id=free.vpn.unblock.proxy.fast.secure.minivpn

Gambar selanjutnya, terdapat banyak sekali pilihan server dari berbagai negara secara gratis, maupun berbayar. Bila berbayar pengguna disini dapat membuka Netflix, padahal saat ini Netflix statusnya diblokir oleh pihak PT. Telekomunikasi Indonesia Tbk (Telkom) lantaran tidak memiliki izin atau tidak sesuai dengan aturan hukum di Indonesia. Jika menggunakan VPN tentu hal itu bisa dilakukan dengan sangat mudah karena pemerintah tidak bisa mengawasi kegiatan berselancar internet oleh pengguna.

Terlepas dari hal itu, penggunaan VPN tidak selamanya melakukan hal yang buruk, ada sekitar 31 persen pengguna internet dunia juga memanfaatkan VPN untuk tujuan privasi. Diketahui, informasi pribadi pengguna internet, sangat sering dikumpulkan perusahaan internet guna kepentingannya sendiri. Sehingga menyembunyikan diri melalui VPN untuk privasi merupakan langkah yang baik untuk terhindar dari jebakan perusahaan yang mengambil keuntungan dari VPN. Merujuk dari pendapat Wired, dari penelitian yang dilakukan *Australia Commonwealth Scientific and Industrial Research Organization*, diketahui bahwa 80 persen VPN, terutama VPN mobile (VPN yang khusus dibuat untuk perangkat bergerak seperti ponsel pintar) memiliki masalah perihal enkripsi.[11] Sebanyak 80 persen dari 283 VPN tidak melakukan enkripsi sama sekali atas layanan yang mereka tawarkan. Hal ini sesuai dengan gambar yang ditampilkan sebelumnya yang mana tidak memerlukan enkripsi. Padahal dalam pasal 26 ayat 1 PP PSTE menyatakan bahwa:

> "Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu

[11] Ahmad Zaenudin, *"Internet dibatasi, Masyarakat gunakan VPN"*, https://tirto.id/internet-dibatasi-masyarakat-gunakan-vpn-dVVE diakses pada tanggal 4 April 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan."

"The first analytical of 283 Android apps using Android VPN permissions, extracted from a pool of more than 1.4 million apps on the Google Play Store, performs multiple passive and active measurements designed to show security and privacy features and for the behavior of each app. VPN based. Investigate the possible presence of malware, embed third-party libraries, and manipulate traffic, and measure user perceptions of the security and privacy of these applications. Serious security and privacy policies, such as use of secure VPN tunneling protocols, and IPv6 and DNS traffic leaks. We also report several apps actively performing TLS interception. Of particular concern are examples of applications that include suitable Java Script programs, advertising, and for driving e-commerce traffic to external partners".

Hal ini tidak sesuai dengan fungsi utama VPN yakni berkaitan tentang kerahasiaan *(Confidentially)*, dengan menerapkan sistem enkripsi ini, seharusnya tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah. Lebih parahnya, aplikasi VPN mobile yang diteliti meminta akses pada informasi pribadi pada perangkat milik si pengguna. Hal tersebut jelas merupakan kasus privasi yang cukup serius yang harus segera ditangani. Mengingat, secara umum, masyarakat menyangka bahwa VPN merupakan kata lain dari perlindungan privasi.[12]

"Consensus is the best strategy, for the suppression of computer-related crime entails a mixture of law enforcement, technological and market-based solutions. It can be argued, however, that a strict enforcement agenda is usually not feasible because of the limited capacity of the state. It is also feared that overregulation could stifle commercial and technological development".[13]

Salah satu alasan mengapa banyak VPN yang tidak benar-benar memberikan aspek privasi bagi penggunanya adalah fakta bahwa VPN yang tersedia di pasaran, mengusung dua pendekatan berbeda. Pertama, VPN berbayar dan Kedua VPN gratisan. Padahal mengelola sebuah VPN jelas membutuhkan biaya yang tidak sedikit. Narseo Vallina-Rodriguez merupakan peneliti dari *International Computer Science Institute* mengungkapkan, "secara aspek ekonomi VPN gratis tidak masuk akal, karena ketika kamu mulai melihat aplikasi ini, kebanyakan dari aplikasi tersebut tersedia secara gratis, tapi memelihara infrastruktur online sebenarnya sangat mahal."[14]

---

[12] *Ibid.*,

[13] R.G Broadhurst, "Developments in the global law enforcement of cyber-crime", *Policing: an International Journal of Police Strategies and Management*, Australia: Australian National University Vol. 29, no. 3, 2006, hlm. 408-433.

[14] Ahmad Zaenudin, "*Lolos Sensor dengan VPN*", https://tirto.id/lolos-sensor-dengan-vpn-cs4m diakses pada tanggal 4 April 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Penggunaan VPN ini mencuat pada tanggal 22 Mei 2019, tentu pada saat itu keamanannya belum bisa dijamin oleh pemerintah, sebab aplikasi VPN belum mendapatkan izin baik dari Pemerintah maupun ISP. Maka dari itu, penyedia aplikasi VPN harus memiliki izin dari pihak pemerintah dan ISP 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*, sehingga apabila terjadi pelanggaran maupun kerugian, pihak penyedia VPN dapat diberi sanksi dari Pemerintah dan ISP. Kewajiban mendaftarkan platform digital bukanlah hal yang berat selama aturan dan syarat ketentuannya sesuai.

Dalam masalah ini, yang menjadi poin terbesar adalah pengguna aplikasi VPN yang tidak memiliki itikad baik bahkan tujuan dibuatnya aplikasi itu adalah untuk melakukan kejahatan atau pelanggaran sehingga akan percuma jika pemerintah melanggar tetapi pengguna bisa leluasa membuka situs terblokir dimanapun dan kapanpun. Pihak *Google Playstore* yang mendistribusikan aplikasi yang illegal kurang melakukan pengujian secara massif, sehingga aplikasi illegal bisa saja leluasa tersebar.

Langkah yang dilakukan pemerintah Indonesia khususnya Kominfo berkaitan dengan kasus ini ialah dibuatnya suatu peraturan perizinan aplikasi *Virtual Private Network* untuk mencegah penyebaran berita palsu atau hoaks pada masyarakat. Tetapi peraturan tersebut hanya untuk diperuntukkan bagi VPN yang belum mendapatkan izin dari ISP karena layanan VPN pasti tersambung dengan layanan internet lainnya. Maka dari itu, rencana Pemerintah ialah mewajibkan untuk mendaftarkan aplikasi VPN tersebut ke Pemerintah bila ingin digunakan di Indonesia. Adapun upaya yang dapat dilakukan pihak *Google* dalam menyikapi aplikasi yang merugikan masyarakat ialah mengembangkan model dan teknis pendeteksi yang dapat mengidentifikasi pengembang yang berulangkali melakukan pelanggaran aturan dan jaringan pengembang yang jahat bernama *Google Play Protect*. *Google Play Protect* memindai 50 miliar aplikasi setiap hari. Semua aplikasi Android melewati pengujian keamanan ketat sebelum ditampilkan di *Google Play Store*. *Google Play protect* memeriksa developer aplikasi di *Google Play* dengan sangat hati-hati dan menangguhkan developer yang melanggar kebijakan *Google*. *Google play protect* bertujuan untuk pengguna android agar dapat mengontrol keamanan smartphone mereka sendiri. Cara kerja *Google Play Protect* ini ialah:[15] Memeriksa keamanan pada aplikasi dari google play store sebelum pengguna mendownloadnya; Memeriksa perangkat untuk mendeteksi aplikasi yang berpotensi membahayakan dari sumber-sumber lain seperti malware; *Google play protect* memperingatkan apabila mendeteksi aplikasi yang berpotensi

[15] Layanan Google, Membantu melindungi dari aplikasi berbahaya dengan Google Play Protect, https://support.google.com/googleplay/answer/2812853?hl=id , diakses pada 07 Agustus 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

membahayakan dan menghapus aplikasi tersebut dari perangkat; *Google Play Protect* memperingaktkan pengguna tentang aplikasi terdekteksi yang melanggar kebijakan *software* yang tidak diinginkan dengan menyembunyikan informasi penting atau keliru; *Google Play Protect* mengirimkan pemberitahuan privasi tentang aplikasi yang dapat memperoleh izin pengguna untuk mengakses informasi pribadi anda, yang melanggar kebijakan *developer google*.

Jadi, pengguna bisa mengetahui bahwa Google telah memeriksa dan menyetujui aplikasi tersebut, bahkan sebelum aplikasi tersebut diunduh. Hal ini merupakan suatu upaya yang baik bagi pengguna android dalam menyikapi aplikasi yang illegal digunakan.

Tanggung jawab pengembang Aplikasi terkait dapat diaksesnya situs terblokir oleh Pemerintah

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 No. 11 Tahun 2008 tentang Informasi dan Transaksi elektronik (UU ITE) yaitu sebagai Penyelenggara Sistem Elektronik. Berdasarkan pasal 15 UU ITE, 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.

Dalam Pasal 5 Peraturan Pemerintah Republik Indonesia No. 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik (atau yang disingkat dengan “PP PSTE”) yang menyatakan bahwa Penyelenggara Sistem Elektornik wajib memastikan sistem tidak memuat, memfasilitasi informasi yang dilarang.

> *“According to this rule, the user or programmer will be held liable whenever damage is occurred without having to demonstrate fault or address whether the*

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

> *user failed to take a required level of care, or whether the damage could have been expected or avoided. this rule is accompanied by the principles of reasonableness and good faith which may play a role in ensuring that such a rule will only be applied to the extent necessary to protect the confidence of the other contractor without any extensiveness or exaggeration in that".*[16]

Dalam Surat Edaran Menteri Kominfo No. 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 No. 03 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten melalui Internet *(Over the Top)* diantaranya:[17]

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

[16] Emad Abdel Rahim Dahiyat, "Towards new recognition of liability in the digital world: should we be more creative?, *International Journal of Law and Information Technology*, Vol. 19 No. 3, Oxford University Press 2011, pg. 228.

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

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

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*[18] 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 PP 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 PP 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 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

[18] 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 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

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.

Dalam konteks penyelenggaraan sistem elektronik, pasal 15 dan pasal 16 UU ITE, memberikan standar pertanggungjawaban yang bersifat *presumed liability* karena tidak mungkin pengguna dapat membuktikan kesalahan yang terjadi pada sistem tersebut, karena sistem tersebut adalah teknologi tinggi (*hi-tech)* yang tidak mungkin dapat dengan mudah mengakses dan mengetahui bagaimana substansi sistem tersebut sebenarnya. Maka prinsip yang dapat diterapkan adalah tanggung jawab mutlak (*strict liability*). Penerapan *strict liability* dalam sistem informasi memperlihatkan dua hal, yakni:[19]

1. Terhadap tanggung jawab produk perangkat keras karena dapat dikategorikan sebagai barang (*goods*) dapat dilakukan penerapan prinsip *strict liability (strict product liability)* dengan mudah,
2. Terhadap tanggung jawab atas data, perangkat lunak (*software*) atau tanggung jawab terhadap jasa yang digunakan.

Selain tanggung jawab penyedia, pihak Pemerintah dapat melakukan upaya preventif terkait penyalahgunaan VPN yakni menggunakan pendekatan *Prevention Situation Crime. Pendekatan Prevention Situation Crime* adalah pendekatan yang berfokus pada meningkatkan kesulitan dan mengurangi apa yang didapatkan pelaku. Teori ini memiliki beberapa teknik yang bisa dibedah untuk digunakan sebagai upaya preventif dalam menangani penyalahgunaan VPN, antara lain:[20]

1. Sasaran pengerasan adalah sebuah cara untuk mengurangi peluang pidana seperti penggunaan kunci yang berarti pemerintah bisa memberikan kunci terhadap penggunaan VPN di Indonesia dan bisa dikatakan bahwa penggunaan VPN yang terlalu mudah didapat seperti di google play store. Tetapi alangkah baiknya jika diberikan kunci atau di blokir.
2. Kontrol akses, yakni memberikan pengaman agar penyalahgunaan VPN tidak bisa terjadi dan pengaman tersebut dilakukan dengan cara memblokir akses

[19] 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

[20] 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 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

seseorang yang tanpa izin dan wewenang menggunakan VPN agar tidak bisa menggunakan VPN yang beredar di google play dan app store Indonesia.

3. Kontrol fasilitas yaitu, dapat diartikan bahwa fasilitas di sekitar sebelum pelaku melakukan kejahatan dapat kita kontrol dan bisa memberikan rasa aman para pelaku pelanggaran dan kejahatan yang dimana bahwa VPN bisa melindungi atau mengganti alamat IP seseorang, disini VPN penggunaannya sangat susah untuk dikontrol karena VPN adalah jaringan yang bersifat privat yang tidak semua orang bisa mengakses. maka dari itu dapat diambil keputusan bahwa dengan diblokirnya aplikasi VPN adalah satu solusi terbaik untuk menanggulangi penyalahgunaan VPN di Indonesia dan penghapusan fitur VPN bawaan dari masing-masing smartphone yang beredar di Indonesia harus dihapuskan sebelum beredar di wilayah Indonesia.
4. Masuk/*Screening* keluar sebenarnya sama dengan poin sebelumnya terutama tentang peraturan bagi smartphone yang akan masuk atau beredar di Indonesia agar menghapuskan fitur VPN yang notabene melekat dan tidak bisa dihapus.
5. Mengidentifikasi properti dapat diartikan sebagai pencatatan suatu barang atau alat agar dapat diketahui pemiliknya, jelas disini bahwa teknik ini mendorong agar pemilik alamat IP bisa terdeteksi keberadaannya dan tidak ada lagi keanoniman yang membuat para pelaku penyalahgunaan VPN menjadi bebas berkeliaran, tentu pemerintah sebenarnya sudah melakukan upaya ini yaitu dengan mewajibkan semua masyarakat Indonesia untuk melakukan pendaftaran kartu SIM prabayar mereka, dengan cara itu maka semua data sudah terdaftar di Kementerian terkait yaitu Kementerian Komunikasi dan Informatika, tapi memang upaya itu dinilai tidak akan cukup karena salah satu teknologi VPN yaitu bisa menghalangi atau mengganti provider juga dengan kata lain bila ketika seseorang menggunakan VPN maka bila ditracking maka alamat IP nya saja yang berganti tetapi provider juga akan dipalsukan oleh VPN, maka upaya ini bisa dianggap hanya 50 % efektifnya.

Kasus Tanggal 22 Mei 2019 itu membuat Pemerintah khususnya Kominfo tengah merancang Peraturan salah satu upaya yang dilakukan oleh pemerintah adalah membuat regulasi yang bersifat teknis terkait layanan VPN gratis, hal ini bertujuan agar VPN harus memiliki izin, tetapi Kominfo tidak akan melarang VPN digunakan di Indonesia, walaupun nanti aturan tersebut sudah diterbitkan. Upaya yang dilakukan pemerintah cukup efektif mengingat banyak negara yang secara tegas menyatakan bahwa VPN dilarang digunakan seperti di China maupun Rusia yang telah memberi sanksi tegas apabila warga nya diketahui menggunakan VPN. Seperti di Tiongkok bahwa VPN harus berlisensi alasannya, supaya perusahaan penyedia layanan VPN tidak sembarang beroperasi lintas negara. Semua penyedia layanan VPN pun diblokir. Mereka baru diizinkan beroperasi di Tiongkok jika sudah mendapat lisensi dari pemerintah. Akibatnya, VPN yang bekerja di Tiongkok tidak bisa menembus situs-situs atau medsos yang diblokir negara. VPN berlisensi itu juga tidak bisa menawarkan anonimitas jejak digital sebagaimana VPN pada umumnya, karena berada di bawah kontrol pemerintah. Di Tiongkok, orang-orang

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

yang ketahuan menggunakan VPN "tidak resmi" akan dikenai denda sekitar $145 atau setara Rp 2.000.000.,00 (Dua juta Rupiah).[21]

Apabila penyelenggara sistem elektronik tidak menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan, maka berlakulah Pasal 100 Peraturan Pemerintah Republik Indonesia No. 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik terkait pelanggaran dan dikenai sanksi Administrasi yang berupa: Teguran tertulis; Denda administratif; Penghentian sementara; Pemutusan Akses; dan/atau Dikeluarkan dari daftar.

Adapun ketentuan pidana dalam penyalahgunaan informasi dan transaksi elektronik diatur dalam Pasal 45 (1) Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dengan pidana paling lama 6 (enam) tahun dan /atau denda paling banyak Rp 1.000.000,00 (satu miliar rupiah). Selain itu dalam Pasal 34 ayat (1) yang berbunyi setiap orang dengan sengaja memiliki perangkat keras atau perangkat lunak computer untuk memfasilitasi perbuatan yang dilanggar akan dijerat Pasal 50 UU ITE dengan pidana penjara paling lama 10 (sepuluh) tahun dan denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

Selain itu, apabila melanggar Pasal 36 pelaku akan dijerat Pasal 51 Ayat 2 dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah):

Selain ketentuan pidana, terdapat pertanggungjawaban perdata yang dapat dilakukan oleh masyarakat tertuang dalam Pasal 38 Undang-undang No. 11 Tahun 2008 yakni setiap orang dapat mengajukan gugatan terhadap pihak penyelenggara sistem elektronik yang menimbulkan kerugian.

Upaya lain yang bisa dilakukan apabila ternyata aplikasi VPN illegal yang tersebar di Indonesia berasal dari negara lain ialah melakukan kerjasama internasional dengan negara lain untuk membawa pelaku *cybercrime* agar dapat diadili di negaranya: 1. Ekstradisi dan Deportasi; 2. Bantuan Timbal Balik *(Mutual Legal Assistance)*

Yurisdiksi merupakan hal yang sangat krusial sekaligus kompleks khususnya berkenaan dengan pengungkapan kejahatan-kejahatan didunia maya yang bersifat internasional (*international cybercrime).* Dengan adanya kepastian yurisdiksi maka suatu negara memperoleh pengakuan dan kedaulatan penuh untuk berbagai

[21] Adi Ahdiat, "VPN dilarang di sejumlah Negara, Apa alasannya?" https://kbr.id/berita/052019/vpn_dilarang_di_sejumlah_negara__apa_alasannya_/99420.html , diakses pada tanggal 11 April 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

aturan dan kebijakannya secara penuh. Masaki Hamano dalam tulisannya yang berjudul *Comparative Study in the Approach to Jurisdiction in Cyber space* pada prinsip-prinsip tradisional atau jurisdiksi tradisional yang berkaitan dengan batas-batas kewenangan negara dalam tiga bidang penegakan hukum, yaitu:[22]

Di dalam Pasal 2 Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa setiap orang yang melakukan perbuatan hukum didalam maupun diluar Indonesia, merugikan kepentingan Indonesia, dan memiliki akibat hukum maka akan diberlakukan Undang-undang ini.

Ekstradisi adalah penyerahan seseorang yang disangka atau dipidana karena melakukan kejahatan oleh negara diluar wilayah negaranya dan didalam yurisdiksi wilayah negara yang meminta penyerahan tersebut karena berwenang untuk mengadili dan memidananya. Selain melalui esktradisi bisa juga dengan cara deportasi yang merupakan tindakan mengeluarkan orang asing dari wilayah Indonesia karena keaberadaannya tidak dikehendaki.[23]

Terkait tempat kejahatan terjadi yang tidak memiliki batasan negara (*borderless)*, penanganan yang paling efektif adalah dengan dilakukannya *Mutual legal Assistance* ("MLA") atau bantuan timbal balik dalam masalah pidana sesuai dengan Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana. MLA memungkinkan Aparat Penegak Hukum ("APH") antar-negara bekerja sama dalam rangka permintaan bantuan berkenaan dengan penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan sesuai dengan ketentuan peraturan perundang-undangan negara diminta. Sampai saat ini, Indonesia baru melakukan empat perjanjian bilateral dalam hal bantuan hukum timbal balik ini, yakni dengan Australia, China, Republik Korea, dan Hong Kong.[24] Kerja sama MLA Bilateral dengan Australia diratifikasi dengan UU No. 1 Tahun 1999, dengan China diratifikasi dengan UU No. 8 Tahun 2006, dan dengan Hong Kong dengan UU No. 3 Tahun 2012.

PENUTUP

Virtual Private Network (VPN) *point to point tunneling protocol* (PPTP) yang digunakan untuk mengakses situs terblokir sebagian besar merupakan sistem elektronik yang tidak andal dan tidak aman sehingga bertentangan dengan pasal 15 UU ITE, serta melanggar pasal 34 ayat (1) dan 36 Undang-Undang No. 11

[22] Barda Nawawi Arief,"Sari kuliah Perbandingan Hukum Pidana", Jakarta: Raja Rafindo Persada, 2002, hlm 246.

[23] Undang-Undang No 1 Tahun 1979 tentang Ekstadisi, Pasal 1.

[24] 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 2020.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pengembang *Virtual Private Network* (VPN) *point to point tunneling protocol* (PPTP) yang telah menyediakan sistem elektronik yang tidak andal dan tidak aman dapat dimintakan pertanggungjawaban secara perdata maupun pidana berdasarkan pasal 38, pasal 50 dan pasal 51 ayat (2) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

DAFTAR PUSTAKA

Adi Ahdiat, 2019, "VPN dilarang di sejumlah Negara, Apa alasannya?" https://kbr.id/berita/052019/vpn_dilarang_di_sejumlah_negara__apa_alasannya_/99420.html, diakses pada tanggal 11 April 2020.

Aditya Pandji, 2019, "Kominfo Mau bikin Aturan dan izin Khusus Aplikasi VPN", https://kumparan.com/@kumparantech/kominfo-mau-bikin-aturan-dan-izin-khusus-aplikasi-vpn-1rGIlEWcY8f

Alfons Tanujaya, 2019, "Apa itu VPN dan Mengapa VPN membuat Koneksi Internet jadi Aman", https://infokomputer.grid.id/read/12313003/apa-itu-vpn-dan-mengapa-vpn-membuat-koneksi-internet-jadi-aman diakses pada tanggal 16 juni 2019

Ahmad Zaenudin, 2019, "Ramai-ramai Menggunakan VPN, tapi Amankah?" https://tirto.id/ramai-ramai-menggunakan-vpn-tapi-amankah-dYLs, diakses pada tanggal 04 April 2020.

Ahmad Zaenudin, 2019, "Internet dibatasi, Masyarakat gunakan VPN", https://tirto.id/internet-dibatasi-masyarakat-gunakan-vpn-dVVE, diakses pada tanggal 04 April 2020.

Ahmad Zaenudin, 2019, "Lolos Sensor dengan VPN", https://tirto.id/lolos-sensor-dengan-vpn-cs4m, diakses pada tanggal 04 April 2020.

Amirulloh, Muhamad, 2016, *Hukum Teknologi Informasi dan Komunikasi (TIK) sebagai Hukum Positif di Indonesia dalam Perkembangan Masyarakat Global,* Bandung: Unpad Press.

Arief, Barda Nawawi, 2002, *Sari kuliah Perbandingan Hukum Pidana,* Jakarta: Raja Rafindo Persada.

Broadhurst, R.G, 2006, "Developments in the global law enforcement of cyber-crime", *Policing: an International Journal of Police*

Budapest Convention on Cybercrime, www.itu.int

Carlo A.Gerungan, "Tanggungjawab Penyelenggara Sistem Informasi jika terjadi Kegagalan Sistem", *Media Neliti*, Vol. XXI, No. 4,

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

2013,https://media.neliti.com/media/publications/885-ID-tanggungjawab-penyelenggara-sistem-informasi-jika-terjadi-kegagalan-sistem.pdf

Clarke Ronald,V, 1997, "Situational Crime Prevention (successfull case studies)", New York, Harrow and Haston publisher Guilderland, 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

Cindy Mutia Annur, "Ramai Dicari Usai Kerusuhan 22 Mei 2019, ini Sisi Bahaya dari Pemakaian VPN", https://katadata.co.id/berita/2019/05/23/ramai-dicari-usai-kerusuhan-22-mei-ini-sisi-bahaya-dari-pemakaian-vpn diakses pada tanggal 16 juni 2019.

Dahiyat, Emad Abdel Rahim, 2011, "Towards new recognition of Liability in the digital world: should we be more creative?", Oxford University Press: *International Journal of Law and Information Technology*, Vol. 19 No. 3.

Direktorat Sistem & Teknologi Informasi ITB, 2016, "Layanan VPN ITB", https://ditsti.itb.ac.id/layanan-vpn/ diakses pada tanggal 16 juni 2019.

Galih, Yuliana Surya, 2019, Yurisdiksi Hukum Pidana Dalam Dunia Maya", vol.7, no.1. www.Jurnal.unigal.ac.id

Hamzah, Andi dan Suparni, Niniek, 2010, *Pornografi dan Pornoaksi dalam Hukum Pidana: suatu studi Perbandingan,* Jakarta: Penerbit Universitas Trisakti.

Jyothi, Kanuga Karuna, 2018, "Study on Virtual Private Network (VPN), VPN's Protocols And Security", *International Journal of Scientific Research in Computer Science,* Engineering and Information Technology, vol 3, No.5.

Kartiko, Galuh, 2013, "Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional", https://www.journal.trunojoyo.ac.id

Layanan Google, Membantu melindungi dari aplikasi berbahaya dengan Google Play Protect, https://support.google.com/googleplay/answer/2812853?hl=id

Muhadir, Noeng, 1996, *Metodologi Penelitian Kualitatif*, Yogyakarta: Rake Sarasin.

Mukti Winanda dan Rizka Widyarini, 2013, "Web Content Filtering", https://keamanan-informasi.stei.itb.ac.id/2013/10/30/web-content-filtering/ diakses pada tanggal 30 maret 2020.

Nugroho,Wahyu dkk, 2019, "The Prevention of Negative Content by using VPN (Virtual Private Network) towards website that is blocked by the government", Universitas Negeri Semarang, *Indonesia Journal of Criminal Law Studies*, vol.4, no. 2.

Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X; e-ISSN:2579-4663,Vol. 29, No.2, Agustus2020, 148-166

Peraturan Pemerintah Republik Indonesia No. 71 Tahun 2019 Tentang Penyelenggara Sistem dan Jaringan Elektronik.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 19 Tahun 2014 Tentang

Penanganan Situs Internet Bermutan Negatif.

Sunggono, Bambang, 2002, *Metode Penelitian Hukum*, Jakarta: Raja Grafindo Persada.

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

Surat Edaran Menteri Kominfo No. 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia Platform dan Pedagang (*Merchant*) Perdagangan melalui Sistem Elektronik (*Electronic Commerce*) yang berbentuk *User Generated Content* (selanjutnya disebut "UGC").

Teguh Arifiyadi, 2012, "Proses Pencarian Pelaku Kejahatan Transnasional Melalui Interpol", https://www.hukumonline.com/klinik/detail/ulasan/lt4ffae8265d21c/kejahatan-transnasional-cybercrime-/ diakses pada tanggal 07 Agustus 2020.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang- Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang No 1 Tahun 1979 tentang Ekstadisi.

Yudha Pratomo, 2019, "APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa", https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa diakses pada tanggal 04 September 2019.