TALREV

Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

LEGAL LIABILITY RELATED TO UPLOADING VIRTUAL PRIVATE NETWORK (VPN) ACCESS DOCUMENTS OF SITE USERS ON THE SCRIBD PLATFORM

Made Wipra Pratistita

Faculty of Law, Veteran National Development University Jakarta, Indonesia.
E-mail: wipratistita@gmail.com

Abstract: Obtaining information for free is widely done by internet users through downloads on electronic publication sites such as SCRIBD by bartering documents uploaded to the site. The uploaded document can interfere with data security if its contents fall into the criteria of vital information. One example occurs in the case of uploading state documents containing Virtual Private Network (VPN) access information by internet users on the SCRIBD website. Departing from the case, the problem arises when the position of VPN access is vital information, what kind of legal liability can be charged to site users for their actions that upload file documents containing VPN access to SCRIBD. Normative legal research methods with an analytical approach are used by the author in discussing these issues. The laws and regulations on information technology information used by the author as the main source are complemented by books and articles on cyber law as additional sources. The result of this research is that VPN access which is determined as vital electronic information encourages legal liability to the uploader of VPN access documents on the SCRIBD website based on the provisions of the applicable laws and regulations. So that the purpose of this research can provide knowledge related to legal responsibility in maintaining the confidentiality of Virtual Private Network (VPN) access to every electronic user.

Keywords: Access, Virtual Private Network, Vital Information, Uploaded Documents, Legal Liability

INTRODUCTION

It is known that a culture of literacy will have a long life, if it has a healthy library access condition. Libraries play a very important role in the field of science development because libraries are not only used to trace information but also to explore information that can be used as material for research and research development. The need to find information sources effectively in literacy opens up technological development in the way of obtaining information that was previously done through conventional media turning to new media.[1] Changes in the way information is obtained from conventional media to new media have an impact on changes in lifestyle and literacy behaviour of the community as a hybrid or mixing between humans and technology so that the concept of electronic publications was born. The concept of electronic publication offers the acquisition of literacy reading in the form of books, documents, papers in the form of e-reader formats that can be accessed easily and quickly through electronic systems connected to the internet network on personal gadgets.

Along with the development of awareness of the protection of intellectual property rights, electronic publication providers provide restrictions by privatising through paid membership

[1] Purwadi & Irwansyah. (2019). "Peran Public Information Officers dalam Komunikasi Layanan Perpustakaan Digital". *BACA: Jurnal Dokumentasi dan Informasi*, 40(1): 68

access.[2] The privatisation carried out by electronic publication providers certainly changes the habit of accessing information and knowledge that was previously obtained free of charge has now switched to paid membership access. Unfortunately, this concept of paid access is difficult to reach for literacy enthusiasts who have economic limitations, so the concept of literacy barter was developed by electronic organisers. The concept of literacy barter is a concept where anyone can enjoy free access to literacy without having to become a paid membership but on the condition that they have a written work or reading that can be exchanged or bartered with readings that have been published on electronic publication sites. Not infrequently the concept of information barter can be disastrous when site users are unable to sort out which information can be exchanged with that which is prohibited by law so that mistakes in uploading documents containing vital information can result in public access to these documents on electronic publication sites.

Documents containing vital information that are publicly accessible can have fatal consequences such as hacking, fraud, breaches or data security disasters on certain electronic systems that have occurred in one of the upload cases on the SCRIBD website. According to news from the news circulating, it is said that the ransomware disaster at the National Data Centre allegedly originated from the upload of confidential file documents belonging to public agencies containing Virtual Private Network (VPN) access information on the Temporary National Data Centre Service by users of electronic publication sites.[3] The spread of this state document initially started with information provided by an account named @kafiradikalis on Twitter X social media. The account said through his tweet that the cause of the ransomware case at the National Data Centre originated from the act of uploading a letter belonging to a public agency containing a VPN access password by someone with the initials DPA on an electronic publication site called SCRIBD. However, within a short period of time from the viral tweet by account X to the SCRIBD site user account with the initials DPA, who allegedly uploaded a state document containing private VPN access, was deleted by the owner.

Although the account has been lost or deleted, the digital trail of screenshots of file uploads on the SCRIBD site which is currently still spread on social media can be evidence of alleged violations committed by the SCRIBD site user account with the initials DPA against confidential documents uploaded to the SCRIBD site. In the perspective of legal responsibility, everyone who carries out activities using electronic systems must carry out the legal provisions governing the operation of electronic systems.[4] The act of uploading a document into an electronic system can be an act prohibited by law when it is categorised as vital information according to the provisions of the legislation. Unfortunately, the current legislation in Indonesia has not been able to provide the position of VPN access

[2] Muchtar Anshary Hamid Labetubun. (2019). " Aspek Hukum Hak Cipta Terhadap Buku Elektronik (E-Book) Sebagai Karya Kekayaan Intelektual". *Jurnal Sasi*, 24(2): 139

[3] Habib Allbi Ferdian. "Benarkah 'Orang Dalam' Bocorkan Username - Password PDN Sebelum Kena Ransomware?"<https://kumparan.com/kumparantech/benarkah-orang-dalam-bocorkan-username-password-pdn-sebelum-kena-ransomware-234R7w8sYzt>. Diakses pada tanggal 07 September 2024, 10.18 WIB.

[4] Andrew Murray. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. UK: Routledge Cavendish, p. 10

TALREV
Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

information as vital information so that a problem arises that is used by the author through this research, namely how is the position of VPN access as vital information in its regulation in Indonesia? which then when connected to the upload of file documents containing Virtual Private Network (VPN) access information by SCRIBD site users when the position of VPN access is possible to enter as vital information, what kind of legal liability can be claimed by site users for their actions uploading file documents containing VPN access to the SCRIBD platform?

Previous research has examined Virtual Private Network (VPN) such as in research conducted by Wahyu Nugroho in 2019 entitled Prospects for Overcoming Access to Negative Content Using VPN (Virtual Private Network) on sites blocked by the government by the police. This research discusses the handling carried out by the Indonesian National Police against the misuse of VPN applications for access to negative content. Furthermore, research conducted by Achmad Bachtiar Rachman in 2019 entitled 'Efforts to Prevent Abuse of Virtual Private Network (Vpn) Based on Positive Law in Indonesia'. This research discusses the prevention of all content prohibited by law and the government is also authorised to terminate access. And finally, research conducted by Lila Luthfia, Faizin Sulistio, Ardi Ferdian in 2023 entitled Urgency of Vpn Abuse Regulation as an Effort to Enforce Criminal Law in Cyber Space. This research discusses VPN abuse by providing a solution to future VPN regulation based on a comparative study in China by adding restrictions on a connection to a data centre that is outside the jurisdiction of Indonesia. Based on the previous research that has been mentioned which is the difference in this research, the author focuses more on the responsibility of site users for the act of uploading VPN access file documents to the SCRIBD site. Thus, the purpose of this research can provide knowledge related to legal responsibility in maintaining the confidentiality of Virtual Private Network (VPN) access to every electronic user.

METHOD

The methodology used to compile the research in this article is normative legal research, so that the author can analyse the case of uploading Virtual Private Network (VPN) access file documents on the Temporary National Data Center Service by users of electronic publication sites using legal theories related to legal responsibility which are linked to legal norms governing a prohibition on the disclosure of vital electronic information through electronic systems by using legal sources consisting of primary legal sources in the form of laws and regulations related to telematics, and secondary legal sources in the form of: magazines, newspapers, books, and web articles related to information data protection. The legal sources that have been obtained are then analysed by the author descriptively and argumentatively using an analytical approach in the writing process.[5] The research discussion consists of two parts. . First, it analyses the position of VPN access as vital information linked to several regulations that provide criteria for documents or information that are prohibited from being published. Second, it discusses the legal responsibility of

[5] Irwansyah. (2023). *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta : Mega Cakrawala, hlm. 153.

website users related to the upload of Virtual Private Network (VPN) access information documents according to the provisions of Law Number 11 of 2008 concerning Electronic Transaction and Information (ITE) as well as its latest amendment, namely Law No.1 of 2024.

Analysis And Discussion

3.1. VPN Access as Vital Information and its Regulation in Indonesia

The rapid development of technology encourages adjustments to the need to obtain information in a fast time without having regional boundaries. This adjustment is supported by the existence of an internet network that can connect one technology device with technology devices in other places that are far away safely and encrypted using Virtual Private Network (VPN) technology. According to Farly, et al in their research define VPN as a network that is created as a link to a large number of network users.[6] Meanwhile, according to Putra, et al, VPN technology is a tool that can combine technological devices to a local network after connecting through a public network first.[7] Even according to Supendar H., VPN technology allows every user of technology devices to access the local network from outside using the internet.[8] From all these definitions, it can be concluded that VPN technology is used to access local networks via the internet through a special way of working.

The workings of using VPN technology are further explained by Gleeson that VPN is an emulation of a private Wide Area Network (WAN) facility using IP facilities' (including the public Internet, or private IP backbones)[9] which means an extension of the private intranet through a public intertnet network that ensures connectivity and security between the final two communications effectively by changing the IP address, identifying network traffic routes and then connecting them to a secure server in a different location, thus making someone's computer or smartphone in that location. The VPN server has a function to forward the internet connection to the technology device through 3 special mechanisms, namely encryption, authentication, and authorisation. Encryption as a process to convert information into a secret code that can only be decoded by the desired recipient. Authentication as a process to ensure data has reached the intended recipient to ensure the integrity of the recipient of the message and its source. While authorisation as the process of granting or denying access to sources located in the network after the user has been successfully identified and authenticated. With these 3 mechanisms in VPN technology, security in using the internet network is maintained because it is difficult for other parties to find out.

Legally, VPN technology is still seen as a tool that is neutral or has no dangerous threats.[10] Whereas VPN technology is currently widely used by private and public agencies in the function

[6] Kaseger Arthur Farly, dkk. (2017). Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi. Jurnal Teknik Informatika, 11(1): 4

[7] Jordy Lasmana Putra, dkk. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. IJCIT : Indonesian Jurnal On Computer and Information Technoogy, 3(2): 264

[8] Hendra Supendar. (2016). Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. Bina Insani Ict Journal, 3(1): 86

[9] Gleeson, et al. (2000). A Framework for IP Based Virtual Private Networks, RFC 2764, RFC2764 https://www.rfc-editor.org/info/rfc2764, p. 4

[10] Wahyu Nugroho. (2019). *Prospek Penanggulangan Akses Konten Negatif Menggunakan VPN (Virtual Private Network) terhadap situs yang diblokir pemerintah oleh kepolisian*. Skripsi Fakultas Hukum Universitas Sebelas Maret Surakarta.

TALREV
Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

of sharing, sending and receiving information data between one department and another that can be interconnected via the internet network through a special mechanism with encryption, authentication, and authorisation. With VPN technology, data distribution traffic and electronic information exchange can be carried out securely without worrying about the opening of vital information data such as consumer data, public service data and other electronic system-related data. This is because usernames and passwords in accessing VPNs are only held and owned by parties who are given special trust or authority so as to prevent certain parties from infiltrating traffic (network traffic) to destroy data security.

The important role of VPNs in safeguarding network traffic is unfortunately not accompanied by the establishment of regulations that have not imposed VPN access as a criterion for vital information. In fact, there are a number of laws and regulations that have regulated and provided a criteria for documents or information that are prohibited from being published such as :

- individual data as a population document regulated in Law Number 24 of 2013 Amendment to Law Number 23 of 2006 concerning Population Administration,
- patient health history data that is kept confidential by hospitals and professionals engaged in the health sector as stipulated in Law Number 36 of 2009 concerning Health,
- confidential company data regulated in Law Number 5 of 1999 concerning Prohibition of Monopolistic Practices and Unfair Business Competition.
- exempted Public Information issued by public legal entity in the provisions of Law Number 14 of 2008 concerning Information Disclosure,
- data in electronic transaction activities regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

All of these rules indicate that VPN access cannot be categorised as vital information. However, according to the author, information content can be said to be vital if it is determined by the legal subject itself based on legal regulations. In this case, VPN access can implicitly be included as vital information by referring to the subject of ownership. If the subject of ownership of VPN access is a private entity such as a company, then VPN access can be categorised as a corporate secret as in the provisions of Article 23 of Law Number 5 Year 1999 concerning Prohibition of Monopolistic Practices and Unfair Business Competition. This is related to the use of VPN technology in business activities carried out by the company if the access is open to the public, of course, it can result in the fall of important information owned by the company into the hands of competitors so as to cause unfair business competition.[11]

So that VPN access can be kept confidential, the company can make a rule in the form of a company regulation for employees and company management or a Collective Labour Agreement for workers or labourers from third parties to be bound by the obligation not to share VPN access along with the sanctions attached to it as the implementation of contract theory based on the provisions of

[11] M. Ridwan. (2021). "Perlindungan Hukum Terhadap Rahasia Perusahaan Di Indonesia". *Varia Hukum*, 3(1): 39

article 1338 of the Civil Code. According to contract theory, agreements made legally apply as in law.[12] In this case, the obligation to maintain company secrets stipulated in the agreement made between employers and employees who work for the company can be valid as a binding law if it has been registered with the agency responsible for certain fields or ratified by the minister or a designated official based on statutory regulations.

However, the implementation will be different when the VPN access is owned by a legal subject that has the status of a public legal entity. The obligation to maintain VPN access was born based on legal arrangements by the State that determine the status of VPN access as vital or prohibited information, thus encouraging special responsibilities carried out as a principle of good governance by public legal entity.[13] Referring to Article 17 of Law Number 14 of 2008 concerning Information Disclosure, it explains that public legal entity have the right to refuse to publish information or provide information to the public in the event that:

a) information that if provided may endanger the defence and security of the state so that it cannot be provided by public legal entity
b) information that has an interest in the protection of intellectual property rights and protection from unfair business competition,
c) information relating to personal confidential data,
d) information that discloses the will or the contents of an authentic deed on the last will and testament of an individual,
e) information that may harm foreign interests, information relating to natural resources and national economic security,
f) the requested public information has not been controlled or documented and
g) information that is prohibited from being disclosed according to laws and regulations.

Based on these provisions, public legal entity that use VPN technology can make VPN access into documents as exempt information if it has been determined through a consequence test by the Information Documentation and Management Officer. A consequence test that results in an assessment of VPN access documents that meet the criteria in article 17 of Law Number 14 of 2008 can then be designated as exempt information on the List of Exempt Public Information and Public Documentation Within Public Legal Entity. VPN access documents that have been designated as exempt information have confidentiality properties when they become Public Agency information assets that need to be safeguarded through an Information Security Management System established through the Regulation on Information Security Management Systems in the Public Agency Environment by the Chief Officer of the Public Agency based on:

1. Article 92 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions related to Infrastructure Facilities as a Means of Securing Electronic Systems against Vital Information in the strategic sector,
2. Article 44 of Presidential Regulation Number 95 of 2018 concerning Electronic-based

[12] M.S. Alfarisi, dkk. (2023). "Penerapan Kontrak Perjanjian Kerja di Indonesia Dalam Perspektif Kitab Undang-Undang Hukum Perdata (KUHper)". *Legalitas: Jurnal Hukum*, 15(1): 95

[13] Sri Nur Hari Susanto. (2019). "Good Governance Dalam Konteks Hukum Administrasi". *Administrative Law and Governance Journal*, 2(2): 208

TALREV
Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

Government Systems related to Electronic-based Public Services,
3. Article 9 of Presidential Regulation No. 82 Year 2022 on the Protection of Vital Information Infrastructure related to the Implementation of Cyber Security Standards,

With the establishment of the Information Security Management System Regulation, the existence of VPN access documents has a legal position as a Public Agency information asset that needs to be maintained through an information security management system. The Information Security Management System is a security mechanism carried out on the ownership of information assets for the purpose of fortifying information assets from various types of cyber crime threats both from within and from outside based on the principles of integrity, confidentiality, and availability of Information and Communication Technology services.[14] With the existence of an information security management system, it can certainly prevent information assets owned by Public Legal Entity from falling into the hands of the wrong party, causing the impact of losses in the opening of VPN access information to be accessible to the public

3.2. Legal liability for uploading VPN access information documents by site users on the SCRIBD platform

SCRIBD is a form of digital publication platform that provides convenience in publishing information or papers through a site to be enjoyed by the public in its position as a site user account. Information or papers available on the SCRIBD platform can be accessed through two ways, namely becoming a member subscribing to paid access or obtaining it for free by bartering documents or works owned. The option to obtain information by becoming a paid access subscription member, the user account will be charged a subscription fee for accessing the SRICBD site within a certain period of time through a predetermined subscription payment method. Meanwhile, the option to obtain papers or information through free downloads is done by bartering documents. The download process of the desired information can be done with the user must upload files or documents with the number determined by the SCRIBD platform as many as 5 pieces to be bartered with one file or document to be downloaded.

There are terms and conditions provided by the SCRIBD website that need to be understood and agreed by the user account in the form of an electronic upload contract before uploading the document which is often referred to as the uploader agreement. On the SCRIBD website this uploder agreement is contained in the following content: 'We neither guarantee against unauthorised copying or distribution of Your Content nor will We be liable for any unauthorised copying or usage of Your Content'[15], which when translated means that the SCRIBD platform does not guarantee

[14] Tuti Hartati. (2017). "Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013". *KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer*. 1(2): 63-70

[15] SCRIBD. Uploader Agreement. Link : https://support.scribd.com/hc/en-us/articles/210129466-Uploader-Agreement-for-Scribd-andSlideshare?_gl=1%2Atu9lh1%2A_gcl_au%2AMTA2MTMzMDM0Mi4xNzE1MDQ1NjQ0LjMyMjkwNTk5NC4xNzIwMDMyNTcwLjE3MjAwMzI1NzA

against unauthorised copying or distribution of content by user accounts (platform users) and is also not liable for unauthorised copying or usage of content by user accounts. Therefore, once a user has uploaded a document to be bartered on the SCRIBD website, the user account is legally responsible for the upload, not the owner of the SCRIBD website. Unfortunately, the agreement is often not easy to understand by site users, so there are many instances of site users uploading content, documents or information that can become serious legal issues such as in the case of uploading confidential file documents belonging to one of the public legal entities containing Virtual Private Network access carried out by the SCRIBD site user account with the initials DPA.

Before analysing the case, it is necessary to determine the status of the VPN access information document owned by the Public Agency, in this case if it has been included in the List of Exempt Public Information and Public Documentation through a decision made by the Information Management Officer of the public agency, the responsibility of maintaining the confidentiality of the public agency's VPN access information document must be carried out by all parties within the public agency through a code of ethics guideline. However, it is different when there is a public agency policy that includes VPN access information documents as a Public Agency information asset, then confidentiality protection is carried out through Information Security Management arrangements by Public Agency employees who have special authority and code of ethics based on the provisions in Presidential Regulation No. 82 of 2022 concerning Protection of Vital Information Infrastructure and Regulation of the State Cyber and Crypto Agency Number 4 of 2021 concerning Guidelines for Information Security Management of Electronic-Based Government Systems and Electronic-Based Government System Security Procedures.

According to Ridwan Halim, legal responsibility arises as a further result of the legal subject carrying out its role, either as a right, obligation or carrying out the role of power.[16] In the theory of legal responsibility, each subject has an obligation to carry out something or in a certain way that does not deviate from the established regulations. Thus, public trust can be obtained when the framework in the implementation of organisational management is carried out responsibly by paying attention to aspects of legal compliance owned by each subject within the public body. Based on this theory, every official and employee of a public body is obliged to carry out their duties, main points, functions and authorities carried out professionally based on statutory orders. The form of attachment of responsibility for all parties within the public body is by carrying out the mandate of Law No.14 of 2008 concerning public information disclosure in carrying out the mandate. 2008 concerning public information disclosure in maintaining VPN access information documents that are included in the List of Exempt Information by the Information Management Officer of the public agency as well as for Public Agency employees who are given special authority based on the provisions of Presidential Regulation No. 82 of 2022 concerning Protection of Vital Information Infrastructure and Regulation of the State Cyber and Crypto Agency No. 4 of 2021 concerning Guidelines for Information Security Management of Electronic-Based Government Systems and Electronic-Based Government System Security

[16] Ridwan Halim. (1998). *Hukum Administrasi Negara Dalam Tanya Jawab*. Jakarta: Ghalia Indonesia, hlm. 39

TALREV
Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

Procedures, of course, are responsible for maintaining and securing information when VPN access documents become an information asset for the Public Agency.

Referring back to the case of uploading Virtual Private Network access file documents made by the SCRIBD website user account with the initials DPA, it can certainly be analysed regarding its responsibility by looking at the position of the user account as the uploader of the document. If the uploader of the VPN access file is an employee who works for a public body, then in civil service law the action can be categorised into a type of violation of the code of ethics guidelines so that the perpetrator can be subject to administrative sanctions in the form of disciplinary penalties based on the level of violation regulated in the regulations on enforcement of public agency employee discipline. However, if the status is an employee of a company that cooperates with public agencies, there is a possibility of sanctions in the form of termination of employment without severance pay as a result of the company being terminated by the Public Agency with a fine for the losses suffered.

In addition to the sanctions for violation of the code of ethics received by the uploader of VPN access on the SCRIBD website, there are other liabilities such as civil suits and criminal charges that can be brought by Public Legal Entity. The act of uploading VPN access as confidential information to a site by the uploader, according to the author, can be included as an unlawful act as regulated in article 1365 of the Civil Code. What is meant by unlawful acts are human actions that violate laws and regulations and/or violate the principles of decency, accuracy, and prudence, causing harm to other parties.[17] In this case, if the upload of VPN access has an impact on the losses suffered by the Public Agency, the Public Agency can file a compensation claim through the Court for the unlawful act committed by the uploader through a reasonable calculation of the losses suffered.

Meanwhile, the uploader can be criminally prosecuted if his actions fall into the criminal elements in Article 32 paragraph (1) jo, Article 48 paragraph (1), Article 32 paragraph (3) jo, and Article 48 paragraph (3) in Law No. 11 of 2008 concerning Electronic and Transaction Information (ITE) as well as its latest amendment, Law No.1 of 2024, which regulates the prohibition for everyone who without the right to transfer or transmit to result in the disclosure of confidential electronic information to be accessible to the public.[18] In this case, when VPN access has been categorised by the Public Agency as exempt information which has a confidential nature that needs to be maintained as a Public Agency information asset through the Information Security Management arrangement, it becomes a prohibition for anyone who without the right to move or transmit to result in the disclosure of VPN access information which then if this is violated so that the VPN access becomes accessible to the public, the uploader can be prosecuted under the threat of a fine of around 2,000,0000,000 (two billion rupiah) or 5,000,000,0000 (two billion

[17] Rai Mantili. (2019). "Ganti Kerugian Immateriil Terhadap Perbuatan Melawan Hukum Dalam Praktik : Perbandingan Indonesia Dan Belanda". *Jurnal Ilmiah Hukum DE JURE Kajian Ilmiah Hukum*, 4(2): 304

[18] Leonardo Latsiano Dade, dkk. (2024). "Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia". *Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum*, 13(3): 10

rupiah) with a long prison sentence of around 8 or 10 years.

Conclusion

By analysing the provisions of the laws and regulations that have been mentioned in the discussion, indirectly documents containing VPN access can be categorised as vital information if determined by the legal subjects themselves in accordance with legal regulations. Private entity can include VPN access as a company secret with confidentiality responsibilities and sanctions for violations regulated in the form of company regulations or collective labour agreements. Meanwhile, the subject of public legal entities can include VPN access in the List of Exempt Public Information and Public Documentation based on the Decree of the Information and Documentation Management Officer so that VPN access that has been determined as exempt information can have vital properties that need to be kept confidential as a public agency information asset through Information Security Management arrangements with responsibility for maintaining confidentiality and sanctions for violations regulated through code of ethics guidelines.

Accountability for the case of uploading Virtual Private Network access file documents carried out by the SCRIBD website user account can be pursued through disciplinary penalties if proven to have violated the code of ethics guidelines, civil suits if the upload of VPN access causes losses suffered by the Public Agency, and criminal charges if the act of uploading VPN access to the SCRIBD site is included in the elements of the act as stipulated in Law No.1 of 2024 concerning ITE in Article 1. Article 32 paragraph (1) jo, Article 48 paragraph (1), Article 32 paragraph (3) jo, and Article 48 paragraph (3) contains a prohibition for any person who without the right to transfer or transmit resulting in the disclosure of confidential electronic information to be accessible to the public with the threat of criminal imprisonment for as long as 1 year.

Bibliografi / Bibliography

Buku

Andrew Murray. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. UK: Routledge Cavendish.

Irwansyah. (2023). *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta : Mega Cakrawala.

Ridwan Halim. (1998). *Hukum Administrasi Negara Dalam Tanya Jawab*. Jakarta: Ghalia Indonesia.

Wahyu Nugroho. (2019). *Prospek Penanggulangan Akses Konten Negatif Menggunakan VPN (Virtual Private Network) terhadap situs yang diblokir pemerintah oleh kepolisian.* Skripsi Fakultas Hukum Universitas Sebelas Maret Surakarta.

Jurnal

Gleeson, et al. (2000). *A Framework for IP Based Virtual Private Networks*, RFC 2764, RFC2764 <https://www.rfc-editor.org/info/rfc2764>

Jordy Lasmana Putra, dkk. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. IJCIT : Indonesian Jurnal On Computer and Information Technoogy, 3 (2): 260~267,

Hendra Supendar. (2016). Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. Bina Insani Ict Journal, 3(1): 85–98.

TALREV

Volume 9 Issue 2 December 2024: pp 392-402
Copyright ©2024 TALREV. Faculty of Law Tadulako University, Palu, Central Sulawesi, Indonesia.
ISSN: 2527-2977 | e-ISSN: 2527-2985.
Open access at: http://jurnal.fakum.ac.id/index.php/TLR

Kaseger Arthur Farly, dkk. (2017*).* Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (*Secure Socket Tunneling Protocol*) Studi Kasus Kampus Universitas Sam Ratulangi. Jurnal Teknik Informatika, 11(1): 4

Leonardo Latsiano Dade, dkk. (2024). Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia. Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum, 13 (3):10

M.S. Alfarisi, dkk. (2023). Penerapan Kontrak Perjanjian Kerja di Indonesia Dalam Perspektif Kitab Undang-Undang Hukum Perdata (KUHper). Legalitas: Jurnal Hukum, 15(1): 95

M. Ridwan. (2021). Perlindungan Hukum Terhadap Rahasia Perusahaan Di Indonesia. Varia Hukum, 3(1): 39

Muchtar Anshary Hamid Labetubun. (2019). Aspek Hukum Hak Cipta Terhadap Buku Elektronik (E-Book) Sebagai Karya Kekayaan Intelektual. Jurnal Sasi, 24 (2): 139

Purwadi & Irwansyah,. (2019). eran Public Information Officers dalam Komunikasi Layanan Perpustakaan Digital. BACA: Jurnal Dokumentasi dan Informasi, 40 (1): 55–72

Rai Mantili. (2019). Ganti Kerugian Immateriil Terhadap Perbuatan Melawan Hukum Dalam Praktik : Perbandingan Indonesia Dan Belanda. Jurnal Ilmiah Hukum DE JURE Kajian Ilmiah Hukum, 4(2): 304

Sri Nur Hari Susanto. (2019). Good Governance Dalam Konteks Hukum Administrasi. Administrative Law and Governance Journal, 2(2) : 205-217,

Tuti Hartati. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer. 1 (2): 63-70