Legal Protection of Electronic Data is approved by electronics as Regulated in Article 1 (one) Paragraph 9 (nine) of Law No. 19 of 2016 in Conjunction with Law No. 11 of 2008 Concerning Information and Electronic Transactions

[1]Timoteus Natanael Sirait [2]Andrie Gusti Ari Sarjolo, [3]Mori Rajagukguk. [4]Goncalwes Sirait
Nommensen HKBP University Graduate program Magister study of law science program
timo17111995@gmail.com

Abstract The development of an increasingly developing era in a country or in the international world, which is carried out does not involve regulations in the fields of government, economics, and events that occur in developing countries or developed countries in the International World. This development makes it easy for every action or action to become easier for individuals or institutions to do work more easily without having to advance first, accessible via the internet. In the profits will have a disadvantage, the same as security will result in spending the misuse of information by some people who debate in the field of information technology that is generally known as "cybercrime". Crime in cyberspace or in English is called "cybercrime" is a term that refers to activities with computers or computer networks into a tool, target or place that is translated as crime. Related to cyber crime, among others are auction auctions, check falsification, credit card / card credit, trust fraud, freedom of identity, child pornography, violence, and others. The current legal provisions concerning the above matters Rule in law number 19 of 2016 amendments to law No. 11 of 2018 concerning Electronic Information and Transactions, which discusses all articles regarding approval in article 1 (one) paragraph 9 (nine) which contains an Electronic Certificate that reads: "Electronic certificates which are electronic certificates issued. Electronic Signature and identity showing the legal status of the parties in the Electronic Transaction issued by the Electronic Certification Service Provider " While in its implementation at this time, globally around the world known security called SSL (Secure Socket Layer) SSL (Secure Socket Layer) is a security layer to protect transactions on your website with sophisticated data encryption technology.Asking the author to try to discuss how to protect electronic legal data regulated in Law No. 19 of 2016 in conjunction with Law No. 11 of 2008 concerning Electronic Information and Transactions relating to Electronic Certificates with the system of enforcing data security systems imposed by commercial and non-commercial institutions on currently both National and Global, called SSL (Secure Socket Layer)

Keyword : Legal, Protection, Elektronik Data, Elektronik Transaction

1. **Preliminary**

The development of technology makes it easy for every action or action to be more practical for individuals and institutions to do a job more easily without having to face to face directly, but through internet access**.**

In law number 19 of 2016 the amendment to law no 11 of 2018 in article 1 paragraph 2 states that :

> "Electronic transactions are legal actions carried out using computers, computer networks, and / or other electronic media"

As for the other words in the law above it means smartphone, tv, radio, which are generally used by the public at this time

in article 1 paragraph 3 of law number 19 of 2016 amendments to law no 11 of 2018

"Information technology is a technique for gathering, preparing, storing, processing, announcing, analyzing and or disseminating information"

In the profits will have the risk of loss, as well as security will result in the misuse of information by some people who commit crimes in the field of information technology which is generally known as "cybercrime"

2. **Discussion**

There are two forms of website that generally apply globally including:
1. Commercial website

2.1. And non-commercial websites

The author believes that the provisions of the legislation is more directed to commercial websites where the implementation of commercial websites will lead to profit or profit. whereas the non-commercial website only contains information about things in both private and government forms. The general public can not ensure the accuracy of the data released by the website which results in information released only engineering without full accountability.

Provisions internationally in the world in an electronic system which in electronic media is called a Website or "website". A website is a collection of interconnected web pages that are generally on the same server containing

a collection of information provided individually, in groups, or in organizations.

In its development the authors found a basic system of the formation of a website that was originally known as Hypertext Transfer Protocol (HTTP) is an application layer network protocol used for distributed, collaborative, and hypermedia information systems. which is currently known as the Secure Hypertext Transfer Protocol is a secure version of HTTP, namely "HTTPS" The author tries to conduct an interview through a chat system on one of the HTTPS service provider websites namely "https://www.dewaweb.com"

contains the result that HTTPS is secured by a system that is embedded with SSL (Secure Sockets Layer)

1. SSL encrypts data on its website Encryption In the field of cryptography, encryption is the process of securing information by making that information unreadable without the help of special knowledge. Because encryption has been used to secure communication in various countries, only certain organizations and individuals who have an urgent need for confidentiality use encryption. For example, Message Authentication Code (MAC) or digital signature. Another use is to protect against computer network analysis.

2. The party that issues the SSL will be responsible for information leakage and guarantees
3. SSL only applies to paid websites

Global facts about the data that are now starting to be bought and sold are not only used by commercial websites but also non-commercial websites, so how is the legal protection for those whose data has been compromised. So the authors make sure that the globally recognized SSL is the same as the nationally known electronic certificate in Indonesia, which at its main point offers data security in an electronic system To simplify its application the authors provide several examples of differences between the web that is safe and not secure.

a. secure web

1. On the web https://putusan.mahkamahagung.go.id In the left corner of the web there is a gombok which when clicked will issue a certificate of information. The certificate was issued by COMODO RSA Domain Validation Secure Server CA and if we click the issuer statement on the bottom we will automatically be transferred to the website that issued the certificate of information.

b. Unsafe web

1. While on the web www.polisionline.com is engaged in the verification of online stores above the top left corner bearing Not Secure, which means the web is not secure.

In law number 19 of 2016 concerning changes to law number 11 of 2008 concerning information and Electronic transactions Article 1 (one) paragraph 9 (nine) states that:

"Electronic Certificates are electronic certificates containing Electronic Signatures and identities that show the legal subject status of the parties in Electronic Transactions issued by the Electronic Certification Provider"
In this article the security of a system known as "electronic certificates" is subject to certainty. From the above understanding the authors conclude that some of the core parts of electronic certificates include:

1. **Electronic signature**
   In article 1 paragraph 12. It is said that:
   "Electronic Signatures are signatures consisting of Electronic Information that is attached, associated or related to other Electronic Information that is used as a verification and authentication tool"

2. **Electronic Transactions**
   In Article 1 paragraph 2 it says that:
   "Electronic Transactions are legal actions carried out using Computers, Computer networks, and / or electronic media"

3. **Identity of the parties**
   Information that explains the party that made the agreement, wherein the electronic certificate states that the signature consists of electronic information, which in implementation is in accordance with Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Transaction Systems
   In Article 39 paragraph 1 part a:
   "Testing the authenticity of identity and checking the authorization of Users of Electronic Systems conducting Electronic Transactions"

4. **The legal subject**
   Law No. 11 of 2008 concerning Information and Electronic Transactions in the explanation of article 9 states that:
   What is meant by "complete and correct information" includes:

"Information containing the identity and status of legal subjects and their competencies, both as producers, suppliers, organizers and intermediaries"

the legal subject is an electronic signature contained in an electronic certificate that explains ownership by the manufacturer, supplier, organizer or intermediary, which in the provisions of article 1 paragraph 13 uu 19 of 2016 concerning ite states that:

"Signatories are legal subjects that are associated or related to Electronic Signatures" The signatories adopted in this article are all individuals, both individuals and commercial and non-commercial institutions

5. **Organizer of electronic certificates**
   rticle 1 paragraph 10 reads:
   "Electronic Certification Organizers are legal entities that function as trustworthy parties who provide and audit Electronic Certificates"
   Which is further stipulated in Government Regulation No. 82 of 2012 concerning the organizer of systems and electronic transactions
   In accordance with the provisions of the legislation in force no. 19 of 2016 in conjunction with no. 11 of 2008 jo Government regulation 82 of 2012 contains the concern that this electronic certificate contains legal certainty about how to implement the provisions in electronic transactions, which in principle, regulate security on the electronic transaction system.

The author is of the opinion that SSL, which is known globally, is part of an electronic certificate which is more detailed in government regulation No. 82 of 2012 Article 11 paragraph 2 "In the event that there are no Indonesian experts, the Electronic System Provider may use foreign experts" article 89 part b

Electronic System Eligibility Certification issued by foreign institutions that fulfill accreditation in the country concerned, remains in effect until the enactment of the Ministerial Regulation concerning Electronic System Eligibility Certification. Evidenced by the security of websites that are used to secure official sites in Indonesia, one of them is the Supreme Court site, "COMODO" which is a foreign-owned security system company,

3. Closing Conclusion

SSL which is known globally is part of the Electronic Certificate which is regulated in Act number 19 of 2016 jo law no 11 of 2008 jo Government regulation no 82 of 2012, which at present this security is in control of developed

countries in Europe ,. SSL security is the security of a website against securing data traffic, both commercial and non-commercial, an easy way to safeguard data security when making a transaction is to look at the prefix of the website that reads HTTPS where the letter "S" means secure or with the meaning of secured On the website, if the click image is clicked, it will be transferred completely to the website security service provider.

4. **Suggestion**

Indonesia must improve its security in its own technology sector in the process of data security

In the statutory regulations, it should be more detailed in regulating government regulations concerning Secure Sockets Layer

References

Law No. 19 of 2016 concerning information and electronic transactions

Law 11/2008 concerning information and electronic transactions

Government Regulation number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions

The web

https: // dewaweb.com

https://id.wikipedia.org/wiki/ Crime_dunia_maya

https://id.wikipedia.org/wiki/Website

https://id.wikipedia.org/wiki/Protokol_Transfer_Hiperteks

https://id.wikipedia.org/wiki/HTTP_Secure

https://id.wikipedia.org/wiki/Enkripsihttps://id.wikipedia.org/wiki/Encription