Abstract
The Information Technology Revolution, which began with discovering several tools and components related to the digital world in its development, has formed a new world known as cyberspace. Mayantara, as a world characterized by relationships that do not bring the parties together physically, forms its values, norms and concepts. However, the rapid changes produced by technology and information have caused the norms and concepts they have produced to be fully realized. Behind all the conveniences provided through the use of technology and communication, there are several crimes (cybercrime) that are worrying and risk causing harm to several parties, through several social media and the digital world, suspects can move quickly according to their desired interests, both individually or as a group, from several cases of cybercrime that most attract the attention of the public and the general public, the crime of defamation is a case that must be resolved immediately with several strengthening of the criminal law law to the fullest. This study uses a normative juridical method, with a qualitative approach and the results of this study explain that cybercrime cases that occurred in Indonesia have actually been specifically regulated through the electronic information and transaction law, besides that the law can also prosecute these cases. Criminal law, but in the process the handling of cybercrime cannot be carried out optimally. Especially in the crime of defamation, which is carried out through technology and social media, the perpetrators can be charged with articles 310 to 321 and also regulated in Article 27 paragraph (3) of Law No. 11 of 2008. Defamation is an act the dissemination of information that is not true and is usually in the form of slander against someone that has a bad impact on that person, the person whose name is defamed can complain about it for defamation and the person who commits the defamation can be punished with imprisonment and the penalty of paying a fine.

Keywords: Cybercrime, Cyberspace, Indonesia

Introduction
The rapid development of information technology in various segments of human life, of course, can provide benefits and convenience when used in proper corridors, but on the other hand, the emergence of technology and information does not always provide good for
changes in human life, there are times when the bad side of globalization which has a negative impact so that it can harm many people. Nevertheless, it cannot be denied that globalization is one of the factors causing the rapid and unlimited development of technology, besides the emergence of very deep knowledge of various aspects and fields that are managed by humans so that it can provide new understanding and experience that has never been seen before. Felt before, but on this knowledge, not everyone can use it wisely and correctly (Nasi et al., 2015; Makhali, 2021).

In the process, the development of information technology has also at least formed a new world society that cannot be hindered by the boundaries of space and time, with all the convenience and sophistication of information technology that can be used anywhere, humans continue to strive to develop and innovate to improve various the type of technology as a supporting medium which is certainly able to facilitate the work and daily human activities. Along with the rapid pace of development of information technology that humans are feeling in the last few decades, at least it also has an effect on changes in patterns of activity and human life in general, so that it directly affects the emergence of new types of legal acts and events within the scope of human life itself.

Human life in the current era cannot be separated from the role of technology, the rapid growth of technology is directly proportional to the increase in human needs, which cannot be separated from the use of various media, especially in visual media and electronic media, humans as social beings, need tools and equipment. A tool as a result of technology development, namely in the context of communicating and exchanging information, the existence of this technology in principle is indeed functioned as a media service and is expected to be used in a timely, effective, and targeted manner. So we can conclude that information technology is said to meet needs on time if it can be available when needed, so that it requires process to speed up to the stage of its development method (Halder & Jashankar, 2016; Nisa, 2020; Sidiq et al., 2021).

However, behind the advancements provided by technology and information, not a few gave birth to some unrest and crimes that emerged in the form of cybercrime, so that it was very detrimental to many people and had a direct impact on the security system in a state order such as in-office agencies and several other government agencies, for example, the crime of hacking or hacking arising from the negative impact of technological advances. Crimes under the guise of technology and information, especially computers and the internet (cybercrime) have reached the stage of worrying many parties, on other hand the increase in internet users among humans has indeed experienced a significant increase, but it should also be noted that advances in information technology have brought many There is a change in the human mindset, besides that technology also has an effect on the increasingly practical and flexible business world, for that it is necessary for all internet users and communication media users to continue to understand so that they can utilize and use them with full responsibility and prudence (Hardinananto, 2016).

According to data from https://patrolisiber.id/statistics from 2019 to 2021, cybercrime is dominated by some content related to the spread of provocative content, including defamation.
The table above explains that the most cybercrime in Indonesia is in defamation cases, in this case the side of technological development saves a lot of benefits and negative impacts on human life but we need to underline that technology also keeps bad and fraudulent practices when used by irresponsible people, as for some of the fraud and abuse that is presented by technology today including the spread of hoax news, digital terrorism, pornography, blasphemy, copyright infringement, and finally defamation. Therefore, the development of Information Technology today, has a positive impact and a negative impact on the pattern of human life, as for the positive impact of the development of information technology, one of which is making the relationship between humans unlimited, while on the negative side it has encouraged the birth of a new legal regime known as information technology crime (cybercrime), officially the law is used to ensnare suspects involved in electronic transactions.

As one of the countries that have an institutionalized system and basis of legal authority, Indonesia puts all kinds of laws and their violations into Article 1 paragraph (3) which is the result of the fourth amendment to the 1945 Constitution, which is abbreviated to (UUD 1945). , which states that the state of Indonesia is a state of law, and if viewed based on that statement, all aspects of life in this country are regulated and limited by legal norms that apply both in the social, political, cultural, economic, and other fields. For this reason, all problems that arise in the social life environment must be resolved according to applicable law, because basically there are many laws that must run according to their roles and functions based on state laws and believe that the law is intended to protect all Indonesian people (Palit, 2013).

The Criminal Code or what is often referred to as criminal law is the basis of a book containing regulations generally applicable to all Indonesian citizens. -State laws to protect and supervise all interests of the general public, including in tackling various crimes that are present through the use of the world of information and communication, but of the many crimes caused by the presence of technology and information, cases of defamation may become one of its phenomena among humans because this behaviour is increasingly happening on various social media and is entering a very worrying phase. Defamation is

<table>
<thead>
<tr>
<th>Types of Cyber Crime</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provocative Content Spread</td>
<td>4.3</td>
<td>2.4</td>
<td>2</td>
</tr>
<tr>
<td>Online Scam</td>
<td>2.5</td>
<td>4.4</td>
<td>4</td>
</tr>
<tr>
<td>Pornography</td>
<td>3.5</td>
<td>1.8</td>
<td>3</td>
</tr>
<tr>
<td>Illegal Axis</td>
<td>4.5</td>
<td>5</td>
<td>5.8</td>
</tr>
<tr>
<td>Data Theft and</td>
<td>3</td>
<td>2.8</td>
<td>8.9</td>
</tr>
<tr>
<td>Defamation</td>
<td>7</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

Source: Patroli Siber 2021

Table 1 Types of Cyber Crime Indonesia in 2019-2021
known as humiliation, which attacks the good name and honour of someone with no special relationship or connection. Still, as a result of this action, a person can feel cornered or harmed.

As a result of the many cases and the phenomenon of defamation that often disturbs the Indonesian people, the government finally made a firm decision in which the perpetrators could be charged with several severe articles, including through Articles 310 to 321 of the Criminal Code. Both verbal and written insults using defamation, slander, or slanderous complaints are regulated in Article 310 to Article 321 of the Criminal Code. Regarding Broadcasting, Law Number 11 of 2008 concerning Information and Electronic Transactions, as for the type of violation that can lead to cases of humiliation on social media that are offensive or personal attacks on someone and result in damage to good name and honour, because basically from various kinds of pollution good name that occurs both on social media and in other forms, these acts are still classified as cyber crimes or cybercrimes and violations of human rights. Recently, there have been frequent criminal acts of defamation committed by various parties. At the same time, the causes are very diverse and varied, ranging from reporting events in the media, revealing research results, reporting a crime, and other actions that cause the perpetrator to be subject to criminal sanctions. Where the criminal sanction in question is a punishment given to someone because he has committed a crime, where the consequences of his actions cause harm to others (Risca, 2018).

Several previous studies were used as reference material and references in compiling this paper, including research compiled by Ali (2016) with the title defamation through information facilities and electronic transactions (study of the Constitutional Court's decision No.2/PUU-VII/2009) where the results of this previous study explain that the occurrence of defamation offenses is not enough if law enforcement officers only base themselves on someone's complaint that their honor or good name has been attacked (subjective element), but must also be based on community assessments including professional circles and linguists. About the perpetrator's actions. In the context of Article 27 paragraph (3) of the ITE Law, the addition of an element of error, namely malice, is necessary to avoid using the article as a political tool. If the above concept is connected with the Constitutional Court Decision No. 2/PUU-VII/2009, basically the existence of Article 27 paragraph (3) does not conflict with the rights of citizens (applicants), freedom of expression and opinion, and the principle of the rule of law, because the basic philosophy of human rights in Indonesia lies in on the balance between human rights and obligations.

The second study was compiled by Singgi et al (2020) with the title law enforcement against hacking as a form of cybercrime. This study uses a normative legal method and a statutory approach, where the results of this previous study explain that law enforcement against criminal acts The crime of hacking is regulated in Law Number 19 of 2016 amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Perpetrators will be given criminal sanctions in the form of imprisonment and fines for violations in the field of hacking. In addition, efforts to eradicate cybercrime refer to the Information and Electronic Transaction Law carried out with preventive and repressive measures. Therefore, the criminal act of hacking which is included in the realm of cybercrime has been regulated in Article 30 paragraphs (1), (2) and (3) of the ITE Law, while the
punishment is regulated in Article 46 paragraphs (1), (2), and (3) of UU ITE. In this regard, the government has taken various countermeasures in the form of preventive and repressive measures (Sihombing, 2018).

The third study entitled the criminalization of cybercrime in a positive criminal law perspective, this research was compiled by Laksana (2019) with a normative juridical approach, and the results of this previous study explain that from a juridical perspective, especially within the scope of criminal law, the application of imprisonment is still needed. In the criminal system and deserves to be threatened against cybercrime perpetrators in Indonesia. Still, the imposition needs to be limited based on certain principles and requirements and supported by the concept of individualization of punishment. Realistic considerations in society. Types of punishment that are appropriate to replace imprisonment for cybercrime perpetrators in Indonesia are social work crimes and surveillance crimes (Nur, 2020; Yana, 2020).

Furthermore, the latest research was compiled by Dewi (2018) with the title perspective on handling cases of criminal defamation related to the implementation of the right to freedom of expression in terms of criminal law and human rights, using library research methods, and the results of this previous study explained that in From a human rights perspective, the handling of defamation is always associated with the abuse of freedom of expression as regulated in Law 391999 and Law no. 20 of 2000. Therefore, the mechanism for handling human rights violations is always related to defamation, classified as minor human rights violations, not serious human rights violations such as genocide and extraordinary crimes (Extraordinary Crime) according to the statutes.

The progress of the internet world is a necessity that arises from very high technological developments, besides the impacts that it causes are various, on the one hand, it brings a lot of changes and mindsets to human life, but it cannot be denied that it causes several problems and actions. crimes that vary, ranging from fraud, copyright infringement, defamation and several other crimes, for this reason it is important to balance the level of use of information technology with high quality and intellectuality. If it is not balanced with the role of law and the values of High awareness levels of users, will also have an impact on the risk of crime arising from the existence of the world of information and communication or often referred to as cybercrime. Based on the results of the description above regarding some of the problems that arise from the cybercrime crime, the researcher tries to study and explain cases of defamation in the scope of social media, because as a country of law, Indonesia is obliged to implement the system and some of its policies appropriately, especially for every citizen who violates and ignores the rules of the law to cause divisions and disputes.

Method
This study uses a normative juridical method, with an approach based on several legal regulations related to the focus of the problem being developed, as for the explanation of the normative juridical method, a study that tries to explain the legal provisions that apply in legislation, and connected with some of the findings in the field, the next researcher will analyze and compare them through the rules and values that exist in normative juridical law regulations. As for some secondary data obtained indirectly, but the object of research is
sourced from primary, secondary, and tertiary legal materials. In addition, the researcher also collected some data on findings in the field using documentary and literature studies for later qualitative analysis. The use of some of the analytical techniques above is a collection of material or legal literature studied previously. Therefore, it is easier for researchers to provide some important descriptions encountered in the field regarding the topic of the problem that is being sought. The last researcher is to conclude several series of processes that have been done previously (Zaini, 2011).

**Result and Discussion**

**Law Enforcement against Cybercrime**

As we know earlier, cybercrime comes from a very high level of advancement and use of technology. At first, it was seen as a breakthrough in increasing human productivity as a whole. In reality, there are negative loopholes that people can exploit. Irresponsible. The existence of legal instruments that are sourced from the 1945 Constitution provides a basis or guideline for law enforcers to be able to implement every policy and legal steps that will be applied to cybercrime actors, because the formation of legislation in the cyber world comes from the desire of the wider community to obtain guarantees of security, justice, and legal certainty in the fairest way possible. The virtue of cyberlaw itself is binding for every individual to submit and follow all the rules contained therein (Susanto, 2017; Okutan, 2019).

Cybercrime crimes are all criminal acts that use electronic means or with the help of an electronic system, for that all conventional criminal acts in the criminal law code as long as using electronic system assistance or facilities can be categorized as cybercrime crimes. However, in a narrower sense, cybercrime regulation is regulated in Law Number 11 of 2008 concerning Information and electronic transactions as amended by Law Number 19 of 2016 concerning Information and electronic transactions.

With the birth of Law no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is a legal policy issued by the government in responding to a series of cases that arose from the rapid development of criminal acts in the field of electronic transactions in Indonesia. The ITE Law is the first law in the field of information technology and electronic transactions as a product of legislation that is very much needed and becomes the legal basis that lays the foundation of knowledge in the use of information technology and electronic transactions. The ITE Law issuance policy is an effort to overcome crime through criminal law itself (Auliana, 2019).

The presence of the ITE Law can be said to complement the existing Criminal Procedure Code (KUHAP), where this Law can regulate procedural law related to investigations by law enforcement officers such as the police and prosecutors. In addition, the Act also summarizes a new paradigm for law enforcement efforts by paying attention to the protection of the privacy of someone involved in it, the existence of such protection is based on data integrity or data integrity by the provisions of laws and regulations. Then the ITE Law also states that in terms of conducting searches and/or confiscations of electronic systems related to alleged criminal acts, they must be carried out with the permission of the head of the local district court. In Indonesia itself, the problem of cybercrime can also be said
to be starting to be considered as a serious problem, why is that, because with the entry of Indonesia into the era of globalization, especially in terms of its relationship with the cyber world, in various fields of life, Indonesian people are starting to get influenced by the cyber world. Therefore, in recent years several cases have started to emerge, especially crimes related to the world of cybercrime. However, prior to the Electronic Transaction Information Law (ITE), Indonesia’s laws and regulations specifically regulated cybercrime (Guntara, 2020).

The policy for regulating criminal acts in the field of electronic transactions in Indonesia is regulated in the ITE Law which is specific in nature, while the legal policy regarding the provisions for criminal acts in the field of electronic transactions is contained in Article 45 to Article 52 of the ITE Law in conjunction with Article 27 to 37 of the ITE Law regarding criminal acts. For the prohibited land, the contents of Article 27 to Article 37 of the ITE Law are as follows, Article 27 paragraph (1) states that every person intentionally and without rights distributes and transmits and makes information accessible. the Electronic and/or Electronic Document that has a content that violates decency; Article 27 paragraph (2) states that every person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content; Article 27 paragraph (3) states that every person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain insults and/or defamation (Indriani, 2016).

**Legal Position in the Crime of Defamation by the ITE Law**
Handling of criminal acts of defamation that is present through social media is always associated with one's honor and privacy, several cases that often arise in Indonesia are now increasingly leading to a very worrying stage, insulting one's name is subjective. The mechanism has been regulated in the provisions of the Criminal Code (KUHP) in CHAPTER XVI Articles 310 to 321. The qualifications for criminal acts of humiliation or defamation as regulated in Articles 310 to 321 of the Criminal Code vary widely, depending on the elements of the crime as formulated. This also needs to be seen about the nature of criminal acts in general which are essentially violations of norms which are also acts that violate the law, or which only endanger the interests of the law itself (Saragih & Lubis, 2019).

Insult or defamation itself has been formulated in Article 310 paragraph (1) and paragraph (2) of the Criminal Code which reads that whoever intentionally attacks the honor or reputation of a person, by accusing something, which means that it is known to the public, then as a result of his actions, he will be threatened with imprisonment for a maximum of nine months or a fine of a maximum of three hundred thousand rupiahs. And attacking someone's honour so that that person feels cornered and feels his honour has been tarnished without any actual evidence and facts (Supiyati, 2020).

The act of attacking a person's honor or good name by accusing something must be done intentionally; the perpetrator does want the consequences arising from his actions, his honour or good name attacks, namely the other person being addressed. In addition, intentionality here must be directed to all the elements behind it, this type of crime is an act that is carried out intentionally to falsely suspect someone that that person has committed a
criminal act. This intention is intended or intended so that the person is suspected or accused of committing a criminal act. When detailed, the elements of Article 318 of the Criminal Code include (a) intentionally (b) committing an act (c) falsely suspecting a person and (d) that he (as if) committed a criminal act.

The concept of defamation in criminal law regulated in the Criminal Code is based on two important reasons. First, there are basic provisions in the Criminal Code that can be used as basic guidelines for preparing criminal legislation outside the Criminal Code. The aim is to create unity in a harmonious and harmonized criminal system. In a broad sense, punishment means the process of criminal punishment given or decided by a judge. Therefore, the criminal system includes the entire set of legal provisions that govern how criminal law is applied or applied. As for several cases that have occurred in Indonesia related to the problem of defamation, including the case of the Muslim_Cyber account with the perpetrator with the initials HP (23), the admin of the Muslim_Cyber1 Instagram account was arrested for uploading a screenshot of a fake conversation between the National Police Chief Gen. Tito Karnavian and the Head of Public Relations of the Metro Jaya Police. Kombes Argo Yuwono. The contents of the conversation discussed the case of the leader of the Islamic Defenders Front (FPI) Habib Rizieq Shihab. Although, in the snippet of the message, it seems that Tito and Argo are planning to engineer a case to bring down Rizieq Shihab, it doesn't stop there, the @muslim_cyber1 account also contains uploads containing SARA, slander, and hate speech. For his actions, the suspect will be subject to Article 28 paragraph (2) in conjunction with Article 45a of the ITE Law and or Article 4 letter d number 1 in conjunction with Article 16 of Law Number 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination (Simbolon, 2018).

Then there was the case of Muhammad Tamim Pardede, he was arrested for uploading a video on a Youtube channel which contained insults to the President and the National Police Chief, in one of the videos, the suspect stated that Jokowi sided with the communist bloc, and he also stated that the National Police Chief Tito was Jokowi's henchman who believed in communists. In the nearly four-minute video, Tamim Pardede also claims a research professor from LIPI. And after LIPI searched data and facts, it turned out that Tamim Pardede's name was not a research professor from LIPI and this institution never confirmed him as a research professor. But in the end, the Jakarta high court no, 326/Pid.sus/2017 PT. DKI stated that Muhammad Tamim Pardede was a defendant with an alleged defamation case and spreading fake news (hoax).

The scope of the crime of defamation, hate speech, and the spread of fake news are officially included in the realm of criminal acts against one's honor and privacy, other terms used in crimes against honor are criminal acts of humiliation. acts of defamation, hate speech against a person, group or institution based on the Circular Letter of the Chief of Police Number: SE/06/X/2015 contained in article 156 of the Criminal Code, Article 157 of the Criminal Code, Article 310 of the Criminal Code and Article 311 of the Criminal Code. Article 16 of Law Number 40 of 2008 concerning Elimination of Race and Ethnic Discrimination. Article 27 paragraph (3) and Article 28 paragraph (2) of Law no. 19 of 2016 concerning ITE (Syarifuddin, 2018).
The act of defaming a person's honor and reputation which is prohibited by criminal law, the Court institution gives the opinion that criminal law protects a person's good name, dignity, or honor because this is one of the legal interests that are part of everyone's constitutional rights guaranteed by law. The 1945 Constitution, or with international law, because if an act of attacking a person's reputation, dignity or honour is given a criminal sanction, it is not contrary to the 1945 Constitution. Based on the explanation above, it can be concluded that the regulation of the offense of pollution in Article 27 paragraph (3) The ITE Law with the provisions on human rights cannot be separated from the rights of others regarding equal rights and obligations for every citizen to respect the rights of others, so there is a balance between interpreting and implementing human rights. The regulation cannot be categorized as a violation of human rights. Individual rights of citizens (applicant) (Muthia & Arifin, 2019).

Conclusion
Based on the description above, we can conclude that one of the things behind the birth of the ITE Law is the increasing number of crimes in society, especially in the world of technology and information, so the law must also develop so that its function as a security provider can be fulfilled. With this Law, it is hoped that the public will be afraid to make mistakes because as explained in the ITE Law, they are responsible for all losses and consequences that arise. Meanwhile, in some cases of defamation or insults conveyed through social media, it can lead to sanctions and criminal acts contained in the ITE Law with the threat of imprisonment for six or four years, through laws and regulations made to ensnare the perpetrators. In cybercrime, the government takes various measures so that the perpetrators get the appropriate punishment, because after all the presence of information and communication technology in human life must be used and carried out by applicable ethics, norms and morals, for that the most effective way The elegant way to prevent the perpetrators of this Cybercrime is to enforce the law as fairly as possible by the provisions of the Criminal Law Act.

References
Dewi, C. O. (2018). The perspective of handling cases of criminal defamation is related to the implementation of the right to freedom of expression in terms of criminal law and human rights. Lex Et Societatis, 6(4).


