IJCLS 3(1) (2018) 25-34

IJC LS

INDONESIAN JOURNAL OF CRIMINAL LAW STUDIES
http://journal.unnes.ac.id/sju/index/php/ijcls

Existence of Criminal Law on Dealing Cyber Crime in Indonesia

Ranty Mahardika Jhon[1]
[1]*Faculty of Law, Universitas Negeri Semarang, Central Java, Indonesia*

Received February 10 2018, Accepted April 22 2018, Published May 30 2018

DOI: 10.15294/ijcls.v3i1.16945

How to cite:
Jhon, R. M. (2018). 'Existence of Criminal Law on Dealing Cyber Crime in Indonesia", *Indonesian Journal of Criminal Law Studies* 3(1): 25-34. DOI: 10.15294/ijcls.v3i1.16945

Abstract

Cybercrime is a social phenomenon that opens the scientific horizons in the world of law, how a very terrible crime can be done by just sitting sweet in front of the computer. Cybercrime is a dark side of the advancement of information and communication technology that brings widespread implications in all areas of life as they are closely linked to economic crime and organized crimes. From several types of cybercrime, UN Congress X in Vienna established hacking as first crime. The question is whether a positive criminal law can reach cybercrime, there are at least two discourses developed among criminal law experts. First, cybercrime is not a new crime and is still affordable by the Criminal Code to deal with it. In this view the arrangement to deal with cybercrime should be integrated into the Criminal Code and not in its own laws. Secondly, this opinion states the need for renewal of criminal law by forming a new law governing cybercrime. This is based on the fact that this crime has characteristics different from conventional crime, while the existing criminal law instruments are still difficult to cope with the development of this crime. There are two interesting things to look at. First, the development of Information Technology and cybercrime. Second, concerning the existence of Positive Criminal Law in handling cybercrime in Indonesia.
Keyword: Hacking, Cybercrime, Criminal Policy

INTRODUCTION

Utilization of information technology in the global era is currently used by almost all circles, ranging from government to private institution (Sutarman, 2007). One form of development of information technology is the internet. The Internet was originally a study conducted by the Advanced Research Project Agency (ARPA). This network will serve as a communication tool that connects military, university and military equipment manufacturers. The Internet will be an alternative communications infrastructure network if its main network is destroyed in a nuclear attack (Wahid & Labib, 2005).

The Internet is an information and communication space that permeates the

**Email: rantymahardika@gmail.com*
Address: K Building, Kampus Timur, UNNES Sekaran, Gunungpati, Semarang, Central Java, Indonesia, 50229

boundaries of jurisdiction between countries. A medium that offers a variety of transactional conveniences without meeting the parties physically or materially. The Internet has brought us into a new world called cyberspace, which in its development not only bring positive effects but also full of negative impacts. Cyberspace as a computer-based communication medium (computer mediated communication), many offer a new reality in interacting in the virtual world. The interaction between cyberspace users has been dragged towards a deviation of social relations in the form of a distinctive crime that has characteristics different from the conventional crime that has been known. But there is also a view that the crime through the internet (cybercrime) has similarities with the form of crime in the real world.

Sahetapy explained that crime is closely linked to the advancement of information technology and the level of modernization of a nation. This means that the higher level of information technology utilization and the more modern a nation, the more modern the level of crime that arises, both about the nature, form, type, and how the implementation (Wahid, 2002). Cybercrime is a dark side of the advancement of information and communication technology that brings widespread implications in all areas of life especially closely linked to the economic crime (Souka, 1999).

Crime in the field of information technology in general can be categorized into two groups. First, ordinary crimes that use information technology as a tool to help. In this crime there is an increase in modus operandie from the original using ordinary equipment, now has been utilizing information technology. The impact of ordinary crimes that have used information technology has had a serious impact, especially when viewed from the reach and value of the losses incurred by the crime. The theft of money by bank burglary or the purchase of goods using a stolen credit card through the internet media can claim victims in the jurisdiction of another country, a rarity in conventional crime. Second, the crime that comes after the Internet, where the computer system as a victim. Crimes that use internet applications are one of the developments of information technology crime. The types of crime in this group are increasing as the information technology progresses. Examples of this group's crime are the destruction of Internet sites, the transmission of viruses or computer programs that aim to damage the computer's work system (Sutadi, 2003).

Types of computer-related crime activities are very diverse, so many new terms emerge include: hacking, cracking, viruses, booting, trojan horse, spamming, and so forth. However, in order to narrow the scope of the discussion, the author only limiting and raising legal issues surrounding law enforcement of hacking crimes in terms of criminal justice policy in Indonesia. Hacking is also known as computer trespass, which is unlawful action any form of reason and motivation. Not infrequently this action is accompanied by fraud, theft, embezzlement or destruction. The hacking crime has had a long history of travel, beginning at the end of World War II until the 60's computer is still a rare item, only a few departments and large organizations have computers.

With the enactment of Act No. 11 Year 2008 on Information and Electronic Transactions (UU ITE) has provided a legal umbrella for activities related to electronic media and cyberspace. The ITE Law is the legal basis of the use and recognition of electronic documents as valid evidence in electronic transactions (Santosa, 2008). Based on the aforementioned thinking, the writer feels the need to write about criminal law policy in handling of the cybercrime.

Based on background above, the problems are how is the development of Information Technology and Cybercrime? And how is the existence of Positive Criminal Law in handling the cybercrime in Indonesia?

RESEARCH METHOD

In legal research there are several approaches, with this approach the researcher will get information from various aspects of the issue that is being tried to find the answer; 1. The method of approach in this research is the approach of legislation (statue approach); 2. A normative study must necessarily use the approach of legislation, because that will be examined are the various rules of law that became the focus as well as the central theme of this research.

FINDING AND DISCUSSION

The Development of Information Technology and Cybercrime

There are two types of crime, namely blue collar crime and white collar crime (Hamzah, 1989). Blue-collar crime, among others, such as robbery, theft, murder, embezzlement and so on, while white-collar crimes such as corporate crime, bureaucratic crime, malpractice, and so on. Sue Titus Reid argues that a crime is a deliberate act of violating a criminal law committed in the absence of a legal or sanctioned defense or justification and sanctioned by the state (Reid, 1979). Sutherland in Soerjono Soekamto argues that the essential characteristic of evil is an act that harms the state and that the state reacts by giving punishment as the ultimate endeavor (Soekanto, Liklikuwata, & Kusumah, 1981).

Along with the development of internet technology (cyberspace) led to the emergence of a crime called cybercrime or crime through the internet network In this computer crime made possible the offense formal and material offense. Formal offense is the act of someone entering someone else's computer without permission, while material offense is an act that causes harm to others (Irmar, 2014).

Andi Hamzah provides a definition of computer crime is defined as the illegal use of computers (Hamzah, 1989). Cyberspace as a computer- based communication vehicle (Baskara, 2001), many offer a new reality in interacting in cyberspace. The existence of interaction between cyberspace users has been dragged towards the misappropriation of social relations in the form of a typical crime that has characteristics different from conventional criminal acts that have been known. But there is also a view that crimes through the Internet have similarities with the form of crime in the real world.

As explained above, in general, cybercrime can be categorized into two groups. First, ordinary crimes that use information technology as a helping instrument. In this crime there is an increase in modus operandie from the original using ordinary equipment, now has been utilizing information technology. The impact of ordinary crimes that have used information technology is quite serious, especially when viewed from the reach and value of the losses incurred by the crime. The theft of money by bank burglary or the purchase of goods using a stolen credit card through the internet media can claim victims in the jurisdiction of another country, a rarity in conventional crime. Second, the crime that comes after the Internet, where the computer system as a victim. Crimes that use internet applications are one of the evils of information technology crime. The types of crime in this group are increasing as the information technology progresses. An example of this group's crime is the destruction of internet sites, the transmission of viruses or computer programs that aim to damage the computer's work system (Sutadi, 2003). Based on the motive of the crime he committed, cybercrime can be classified into two types: (1) cybercrime as a purely criminal act, and (2) cybercrime as a gray crime (Setiadi, 2005).

The Existence of Positive Criminal Law on Handling the Cybercrime in Indonesia

With the advent of information technology, it allows anyone to have legal relationships with other people in any part of the world. The consequence of these advances required laws to regulate human behavior, solving emerging problems, as social control (Mas, 2004). The problem is the speed of the law is not in line with the speed of globalization and information technology, so the impression that the law is always left behind in regulating the activities of human behavior. Lack of law is not an indication that the law is marginalized, but there are some things that cause. First, there is a difference in the interests and political will of the law-making institution (Wignyosoebroto, 2008).Second, the process of legislation takes long time (Chambliss & Seidman, 1971), whereas the development of technology is running so fast that with such a long process the law that formed becomes obsolete from the technology side. Third, the law requires certainty and accuracy, so that the substance or material to be regulated can be used by law enforcers as well as by those who are governed (Friedman, 2012).

The problems that arise between law, information technology and globalization culminate in a single point that is human. Because talking about legal issues is not merely normative but rather deals with human issues. Therefore the most basic legal issue is the human problem (Warasih, 2005). Man is a monodualist being as an individual and a social being (Sunoto, 1985), so that humanity has a broad dimension, which includes social, law, culture, economy, and so on.

The emergence of cybercrime has become a threat of stability for the government because the government is difficult to compensate crime techniques done with computer technology, especially internet and intranet networks. Therefore, the government needs to pay attention to the security side in the utilization of information technology. To overcome the security disturbance is required law. Because the law is a tool to organize society and meet concrete needs in society (Warasih, 2005). This thinking is in line with Purnadi Purbacaraka and Soerjono Soekanto stating that the law aims to realize the interpersonal peace of life which includes the inter-personal order and the personal interest (Purbacaraka & Soekanto, 1978).

In the connection with the above explanation, security side and legal certainty in the utilization of information technology needs to get attention. To overcome the security disturbance and legal certainty in the utilization of information technology the legal approach is absolutely necessary. Act No. 11 Year 2008 on Information and Electronic Transactions, is expected to improve the effectiveness and efficiency of public services and open the widest opportunity to everyone to advance thinking and ability in the field of use and utilization of information technology optimally and responsibly, in addition to it is also expected to provide a sense of security, fair, and legal justification for users and the implementation of information technology.

Positive law that can be used to handle cybercrime, has been regulated in Act No. 11 Year 2008 especially Article 27 to Article 52, is also regulated in other code, namely: (1) In the Criminal Code in particular Article 282 and Article 311 (dissemination of vulgar photos or film), Article 303 (on online gambling games), Article 331 (on defamation through the internet), Article 335 (threats and extortion by email) (2) of Act No. 36 Year 1999 on Telecommunications, including:

(a) Articles 22 and 50, which provide a criminal penalty for the conduct of the crime manipulating access to telecommunication networks;

(b) Article 38 and Origin 55 which provides a criminal penalty for those who cause physical and electromagnetic interference with the operation of telecommunications;
(c) Articles 40 and 56, provides criminal penalties for those who intercept information through telecommunication networks;
(d) Act No 19 of 2002 regarding Copyright, especially Article 1 Paragraph 8, explains that computer program is a set of instructions embodied in the form of language, scheme, code or other form which when combined with media that can be read by computer will be able to make the computer work to perform special functions or to achieve specific results, including preparation in designing these instructions. Article 30 stipulates that the copyright period for a computer program is valid for 50 years,
(e) Act No. 8 Year 1997 on Company Documents, in particular Article 12, explains that company documents in the form of microfilms, and other media (storage devices, information that is not paper, and has a security level that can guarantee the authenticity of transferred or transformed documents) is recognized as valid evidence, (5) Act No. 20 Year 2001 Concerning Amendment to Act No. 31 Year 1999 concerning Eradication Criminal Acts of Corruption, explains that evidence of evidence shall not only be obtained from the statements of witnesses, letters and statements of defendants as provided for in the Criminal Procedure Code but can also be obtained from other evidence in the form of information that is said, sent, received or stored electronically (email), telegram, telex, faximile, and from document in any recording of data or information that can issued with or without the aid of a means, whether contained on paper, any physical form other than paper, or electronically recorded, in the form of writing, sound, images, maps, designs of photographs, letters, signs, numbers, or perforations of meaning;
(f) Act No. 25 Year 2003 on Money Laundering, in particular Article 2 Paragraph 1 q, explains that one type of criminal act of fraud is done through the internet and Article 38 letter b explains that the information uttered, transmitted, received, and stored electronically with optical instruments or similarly constitutes valid evidence, and
(g) Act No 21 Year 2007 on Trafficking in Persons in Part 29, provides for evidence other than as provided for in the Criminal Code, information that is spoken, transmitted, received or stored electronically with optical devices or similarly and recording data or information that may be viewed , read, be heard, and may be issued with or without the aid of a means, whether contained in paper, any physical object other than paper, or electronically recorded.

If we look closely at Indonesia's positive criminal law based on the provisions of the above-mentioned normative legislation normatively, it is able to deal with the crime of misuse of information technology utilization. Augustine Dawaria, argues that the Internet is only a method, the site can be seen as a house, the data is the same as the property of a person, therefore the law can be enforced despite the old positive law (before the birth of Act No. 11 Year 2008), especially after the passing of Act No. 11 Year 2005 on Information and Electronic Transactions. This law expressly states that for the sake of investigation, prosecution and examination in court, in addition to the provisions set forth in the Criminal Procedure Code and other laws and regulations, electronic information and or electronic documents are legal evidence (Article 44 of Act No. 11 Year 2008). Some examples of cases of cybercrime that occurred in Indonesia, among others, as follows:

1. Hacker, Dani Firmansyah, a consultant for Information Technology (IT) PT Danareksa in Jakarta, on Saturday 17 April 2004 successfully cracked the site

(Craking) National Tabulation Center Election http: www.tnp.kpu.go.id belongs to the General Election Commission (KPU) at Borobudur Hotel in Central Jakarta and changed the names of the parties in it into "unique" names such as Kolor Ijo Party, Mbah Jambon Party, Jambu Party, and so on. Mode by testing the server security system http: www.tnp.kpu.go.id by means of XSS aau Cross Site Scripting and SQL Injection. Evidence: log file cabinet, Yogyakarta cafe server, Danareksa server, KPU server, connection graph in the form of webalizer, saturday cd software, one file box and one computer book. a panel of judges at the Central Jakarta District Court headed by Hamdi SH, at the hearing on Thursday, December 23, 2004, set a sentence of 6 months 21 days to Dani Firmansyah. The punishment is based on Act No. 36 Year 1999 on Telecommunications Article 22c jo. Article 38 jo Article 50 and Subsider Article 406 of the Criminal Code (destroying and destroying goods).

2. Cyber Fraud (CC Fraud), Benny Wong on July 14, 2004 made a transaction in "Batikulan Hardy's Supermarket" Giayar Bali, using City Bank credit card numbered 4541 7900 1413 0605 on behalf of Wahyu Nugroho. At that time the transaction was successful. On the same date, Benny Wong went shopping at Sanur Bali's "Hardy's Supermarket" using four fake credit cards, Mastercard from BNI, Visa from Standart Cartered Bank, and Mastercard and Visa from Citibank. But the transaction failed because Credit Card used known Counterfeit. On September 14, 2004 the Denpasar District Court of Justice led by Chief Justice Arif Supratman SH gave the "gift" to the defendant in the form of a prison sentence of 3 (three) years. Nine later, on June 6, 2005, the Court of Justice of Gianyar Bali District Court led by Chief Justice Gede Ginarsa and Public Prosecutor Ida Ayu Surasmi sentenced the defendant to the same imprisonment for 2 (two) years 8 (eight) months. Overall, the penalty for credit card fraud in Bali is 5 (five) years 8 (eight) months. The Court's verdict on Benny Wong in the Denpasar District Court and the Gianyar District Court, based on Article 263 of the Criminal Code (Falsification of the Letter- Whosoever makes a false letter ...), if such use could cause harm, due to falsification of letters, is punishable by the maximum imprisonment six years).
3. Cybersex (pornography), member of the Cybercrimes Unit of the Jakarta Metropolitan Police Special Crime Directorate, Wednesday, July 28, 2004 at around 11:15 pm, has arrested Johnny Indrawan Yusuf aka Hengky Wiratman aka Irwan Soenaryo from Malang, East Java related to VCD Porn trading case and sex aids through the internet in http: www.vcdporno.com The domain name http: www.vcdporno.com itself is registered in Network solution, LLc 13200 Woodland Park Drive, Herdon, VA 200171-3025, USA. Its domain registered on July 4, 2003 and will end on July 4, 2008 in the name of Lily Wirawan Johny Jusuf with address: 20 Sill Wood Place, Sidney, 2171, Australia. The site also has IP Addres: 69.50.194.230 registered at ATJEU PUBLISHING, LLC 5546 West Irma, Glendale, AZ, United States. The defendant shall face a sentence of imprisonment for a maximum of 2 (two) years 8 (eight) months, for violating Article 282 of the Criminal Code (Crime Against Decency).

In the see of the normative review, the laws set forth in the legislation as mentioned above have actually been able to address the problem of misuse of

information technology crime, yet if it is examined from a sociological perspective that says law is part of its social environment, the work of that law is greatly influenced by other social sub-systems such as social, cultural, political, and economic. Similarly, when discussing the law as a system, then the legal norms set forth in the legislation is only a part of another subsystem, the legal structure and legal culture. Therefore, these legal norms can work well if the legal institutions created by the legal system provide support for the workings of existing legal norms and the institutions are able to provide legal services regularly in accordance with the wishes of the community. In addition to being supported by the existing legal structure, it must also be supported by public awareness to implement the law.

Given that cybercrime is a new form of crime, then in criminal law enforcement against the crime, there are still many obstacles. These constraints include: (1). Electrical evidence factor, (2). Factor of the weakness of mastery Information technology and its equipment for law enforcement, (3). Facilities and infrastructure factor, (4). The factor of difficultness is to present the victim, and (5). The factor of the weakness of public legal awareness.

Electrical Evidence Factor. Electric evidence in the form of data and programs in the computer easily changed manipulated, duplicated, deleted and moved. Therefore, it is feared that if necessary in the hearing it is no longer appropriate with the conditions at the time of the incident, whereas in the evidentiary system in Indonesia the evidence must be presented at the hearing.

Factor of the weakness of mastery Information technology and its equipment for law enforcement. In interpreting cybercrime, there may be different interpretations between investigators, public prosecutors and judges, leading to legal uncertainty for justice seekers. This is motivated by still at least law enforcement officers (investigators, prosecutors and judges) who master the ins and outs of information technology (internet).

Facilities and infrastructure factor. In general, computer facilities owned by law enforcement officers are still limited to the needs of operators, not equipped with facilities that can be used to access to the internet. Such conditions greatly affect the performance of law enforcement officers in law enforcement Cybercrime. Law enforcement officers need information that can be accessed through the internet network. For this purpose, law enforcement officers should be provided with education and training on information and communication technology.

The factor of difficultness is to present the victim. Cybercrime whose victims come from abroad is very difficult to be examined, whereas in the existing procedural law should be examined on the victim, as a witness in accordance with the evidentiary system, because the testimony of the victim's witness is one of the evidences to be poured in the minutes of the examination. For victims of cybercrime originating from other countries that have no bilateral relationship with the Indonesian government is difficult to be presented for review. Consequently, it can hamper its typical settlement.

The factor of the weakness of public legal awareness. The participation of citizens in law enforcement efforts against cybercrime is very important. This is to determine the nature of the reproach and the public denial of an act of cybercrime. The legal awareness of Indonesian society in responding to cybercrime activity is still weak. This is due to lack of understanding and knowledge of the community on the type of cybercrime activities. This condition causes cybercrime prevention efforts to experience obstacles. The emergence of cybercrime has become a threat of stability for the government because the government is difficult to compensate crime techniques. Because the law is a tool to organize society and meet concrete needs in society (Warasih, 2005). This

thinking is in line with Purnadi Purbacaraka and Soerjono Soekanto stating that the law aims to realize the interpersonal peace of life which includes the inter-personal order and the personal interest (Purbacaraka & Soekanto, 1978).

The realization of a goal in accordance with the desired can not be separated from the existing system. In a system contains several basic notions, among others include: (1) the system is always goal-oriented, (2) the whole is more than just the number and its parts, (3) the system always interact with the larger system that is its environment, and (4) the operation of parts of the system creates something of valuable (Shrode & Voich, 1974).

CONCLUSION

Cybercrime is a dark side of the advancement of information and communication technology, which brings immense implications in all areas of life especially closely related to economic crime. Based on the motive of the crime he committed, cybercrime can be classified into two types: (1) cybercrime as a purely criminal act, and (2) cybercrime as a gray crime. The development of cybercrime in Indonesia from year to year has increased, along with the increasing number of internet users. In this regard it is absolutely necessary to consider how to overcome it. Judging from the normative review of positive criminal law and supplemented by the birth of Code No 11 of 2008 on done with computer technology, especially internet and intranet networks. Therefore, the government needs to pay attention to the security side in the utilization of information technology. To overcome the security disturbance is required law.

Information and Electronic Transactions, able to deal with cybercrime. Judging from the empirical review of crime prevention for cybercrime in Indonesia have many obstacles. This is due to, among others, the existence of electric evidence factor, the weakness of the mastery of information technology and its tools for law enforcers, lack of complete facilities and infrastructure available, the difficulty of bringing the victims and the weakness of legal awareness of the community. In order to deal effectively with cybercrime crime, then: All law enforcement officers need to be provided with education and training related to the ins and outs of information technology (internet); Education to the community about the profit and loss of cybercrime should continue to be done, including education about the legal sanctions; Computer facilities owned by all units of law enforcement officers must be equipped with programs that can be used to access the internet, it is necessary to increase bilateral cooperation with other countries, especially with neighboring countries. The competent authorities need to be more careful about hidden foreign agendas in the technical aspects of the internet banking implementation, as related to software recognition and certification authority until now we are still dependent on foreigners.

BIBLIOGRAPHY

Baskara, Tubagus Rony Rahman Niti. (2001). *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*. Jakarta: Peradaban.

Chambliss, William J & Robert B. Seidman. (1971). *Law, Order and Power*. Reading: Mas Adisson – Wesly.

Friedman, Lawrence M. (2012). *The Legal System a Social Science Perspective,* Alih bahasa M. Khozim. Bandung: Nusa Media.

Hamzah, Andi. (1989). *Aspek-aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika.

Irmar. (2014), *Online,* retrieved from www.irmarr.staff.gunadarma.ac.id, accessed on 26 November 2014.

Mas, Marwan. (2004). *Pengantar Ilmu Hukum*. Jakarta: Ghalia Indonesia.

Purbacaraka, Purnadi & Soejono Soekanto. (1978). *Perihal Kaidah Hukum*. Bandung: Alumni.

Reid, Sue Titus. (1979). *Crime and Criminology*. New York: Hot Rinehart and Winston.

Santosa, Agus. (2008). "Perjalanan Panjang Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektonik". *Buletin Hukum Perbankan dan Kebanksentralan*. Volume 6. Nomor 1.

Setiadi. (2005). "Penegakan Hukum terhadap Pelaku Tindak Pidana Internet Banking". *Jurnal Hukum Teknologi*, Volume Nomor 1 Tahun 2005.

Shrode, William A. & Dan J.R Voich. 1974. *Organication and Manajement Basic System Concept*. Tilahassee: Florida State University Press.

Soekamto, Soerjono Hengkie Liklikuwata, dan Mulyana W. Kusumah. (1981). *Krimonologi Suatu Pengantar*. Jakarta: Ghalia Indonesia.

Souka, Mark. (1999). *Ruang yang Hilang Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*. Bandung: Mizan.

Sunoto. (1985). *Mengenal Filsafat Pancasila, Pendekatan Melalui Etika Pancasila*. Yogyakarta: Hanindita.

Sutadi, Heru. (2003). 'Cybercrime, apa yang bisa diperbuat?', *Online,* retrieved from http://www .sinarharapan.co.id/berita/0304-05-opi01.html.2003 , accessed on 26 November 2014.

Sutarman. (2007). *Cybercrime Modus operandi dan penanggulangannya*. Yogyakarta: LaksBang PRESSindo.

Wahid, Abdul. (2002). *Kriminologi dan kejahatan Kontemporer*. Malang: Lembaga Penerbitan Fak Hukum Unisma.

Wahid, Abdul, dan M Labib. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung : PT Refika Aditama.

Wignyosoebroto, Soetandyo. (2008). *Hukum dan Masyarakat*. Malang: Bayu Media Publishing.

Warasih, Esmi. (2005). *Pranata Hukum Sebuah Telaah Sosiologi*. Semarang: PT. Suryandaru Utama.