Published by: Institute of Computer Science (IOCS)

International Journal on Social Science, Economics and Art

Journal homepage: www.ijosea.isha.or.id

Rationalization of technological criminology in the era of disruption

Supardi Hamid
Ilmu Kepolisian, Sekolah Tinggi Ilmu Kepolisian (STIK) Jakarta, Indonesia

Article Info

Article history:

Received: Jan 28, 2023
Revision: Feb 14, 2023
Received: Feb 28, 2023

Keywords:

Criminology;
Disruption;
Technology.

ABSTRACT

In this era of disruption, the crime of manipulating electronic information, fraud, forgery or engineering using computer networks or the internet continues to grow. This study aims to examine the Rationalization of Criminology in Technology in the Disruption Era and Legal Reformulation in Preventing the Formation of Patterns of Criminological Rationalization in the World of Technology in the Disruption Era. With the formulation of the problem, namely the Rationalization of Criminology in the World of Technology in the Disruptive Era. Law Reformulation in Preventing the Formation of Criminological Rationalization Patterns in the World of Technology in a Disruptive Era. This research is a normative legal research with a statutory approach taken from secondary and tertiary data, which is then analyzed. The results of this study found that technology in the current era of disruption has significantly increased legal issues. So there is an urgency to carry out mapping as soon as possible to study criminology, which continues to this day. The contribution of this study is to provide an understanding and analysis of the problems related to the impact of the era of disruption and the influence of technology on the behavior of individuals and complex societies, so as to provide a basis for the government to reformulate the law more specific and detailed to prevent the formation of criminological rationalization patterns.

Corresponding Author:

Supardi Hamid,
Ilmu Kepolisian,
Sekolah Tinggi Ilmu Kepolisian (STIK) Jakarta,
Jl. Tirtayasa Raya No.6, RT.9/RW.4, Melawai, Daerah Khusus Ibukota Jakarta 12160, Indonesia
E-mail: supardihamid@stik-ptik.ac.id

1. INTRODUCTION

The definition of rationalization that can be applied in this study is the process, method, action (according to the ratio) or making the ratio right (good). (*Search Results - KBBI Online* , nd). By fabricating the justifications for their own behavior after the fact, people engage in the process of rationalization. After that, people's own expectations and motivations are typically reshaped to conform to the fabricated ones.(Cushman, 2020).

Meanwhile, in general we can define what criminology is derived from the word crimen which means crime and logos which means science, so that criminology is the study of crime and criminal acts (Sururiyah, 2017) . So that criminological studies can be grouped into four aspects of discussion including crime, perpetrators of crime, victims of crime, and society's reaction to crime. In addition, when viewed from a historical perspective, the name criminology was first discovered by P.Topinard

(1830-1911), a French anthropologist, literally criminology comes from the word "crimen" which means crime or crime and "logos". " which means science. Criminology can mean the study of criminals and crimes (Alam & SH, 2018) .

Technology is a scientific method to achieve practical goals. applied science which is the overall means of providing the goods needed for the continuity and comfort of human life. (Rahmadsyah et al., 2021) . Furthermore, in the Big Indonesian Dictionary, disruption is defined as being uprooted from its roots (*Search Results - KBBI Online* , n.d.) . If interpreted in everyday life, disruption is a fundamental or basic change, namely the evolution of technology that targets a gap in human life. Digitalization is the result of the evolution of technology (especially information) which has changed almost all orders of life, including the legal system (Kurniawan, 2019) . The existence of uncertainty and changes that very quickly bring about changes in attitudes in individuals, community groups, symptoms of behavior change begins with the emergence of anxiety in individuals, community groups, organizations and companies. In individuals, the most visible anxiety is anxiety over economic problems, such as job loss and economic downturn.

Anxiety about economic problems has an impact on other problems such as anxiety about family problems, children's school fees, health and family basic needs. This situation will then cause pressure (stress) on the mind and psychology of the individual and have an impact on the paradigm shift of the family and the environment in individual life. The tendency for individualism is an obvious symptom in society (Esturgo-Deu & Sala-Roca, 2010) . Individualist attitude on the one hand can be understood as a reflection of the anxiety they experience, but this attitude also results in an attitude of not caring about the environment. The emergence of this situation makes the environment become indifferent to the social environment around it. In Indonesian society, which generally still has high social cohesiveness (closeness) to the environment, this is a condition that can threaten social life. Existing social values and norms become things that will be threatened through individualistic attitudes.

In addition, in the era of disruption, transactions occur without face-to-face meetings and are replaced by online services. Not only in the form of a more sophisticated information system, social media is also an alternative in increasing sales. This situation makes cyberspace a substitute for situations that are considered practical to represent real world conditions that are starting to be considered impractical in transactions. In terms of social life, the market which was originally used as a place for social interaction was replaced by the virtual world with the help of information technology. Other innovations that have emerged to take advantage of information technology are 3D Printing, Big Data, Bitcoin, Cloud Technology, Internet of Things, MOOCs (Massive Online Open Course) (Dotsika & Watkins, 2017) . The emergence of science that supports the use of information and communication technology also provides space to influence people's behavior. Things that are currently of great concern include behavior that arises as a result of the use of social media which has become part of the style of interaction in society. Mapping this situation can be simplified by providing a limitation that the era of disruption has changed the behavior of individuals and industries which can have an impact on decreasing value in society and causing social vulnerability (Subasman, 2019) .

The following is an analysis of the issues that arise: *Rationalization and Justification of Behavior*, The explains that people often engage in rationalization or making justifications for their behavior. This can cause changes in individuals' expectations and motivations to conform to the justifications they have made. This can be a problem when individuals justify behavior that is inappropriate or violates social norms and values. *Crime and Criminal Acts Criminology*, is the study of crime and criminal acts, including the study of perpetrators, victims, and society's reaction to crime. With the increasingly rapid development of technology, crime and criminal acts can become more complex and difficult to detect or address. *Disruption and Technological Change*, Disruption is a fundamental change in technology that targets gaps in human life. This can cause changes in behavior and lifestyles of society. Digitalization has also changed almost all aspects of life, including the legal system. However, the speed of change can cause uncertainty and anxiety among individuals, groups, organizations, and companies. *Tendency towards Individualism and Decrease in Social Values*, In a society influenced by the era of disruption, there is a tendency towards individualism that can be understood as a reflection of the anxiety experienced. However, this tendency can also result in a lack of concern for the environment. This can threaten social life, as existing social values and norms can be threatened by individualistic attitudes. *Changes in Social Interaction Patterns and Technological Influence,* The use of technology and the internet has changed social interaction patterns and replaced markets or places of social interaction with the virtual world. Technological influence can also affect individual behavior, such as through the use of social media. This can cause changes in behavior and values that can reduce social value and increase social vulnerability.

Issues related to the impact of the era of disruption and the influence of technology on the behavior of individuals and society have significant implications for the need to reformulate existing legislation, as well as the development of new regulations. For example, in terms of rationalization and justification of behavior, it may be necessary to review and update laws related to ethical behavior, such as the code of ethics for professionals, to ensure that they are relevant and effective in regulating behavior in the digital age. This may include the addition of special provisions or clauses that address issues related to the use of technology, social media, and online transactions. Similarly, in the case of criminal acts and criminal acts, it is necessary to update existing criminal legislation to keep pace with technological developments and changes in criminal activity. This can include creating new violations or amending existing ones, such as those related to cybercrime, identity theft, or online fraud.

Regarding the tendency to individualism and the decline in social values, it may be necessary to develop new laws or regulations that promote social responsibility and accountability, such as those related to environmental protection or community service. This can include the imposition of new sanctions or sanctions on behaviors that harm the environment or society, as well as the promotion of alternative behaviors that are more socially responsible. Overall, the impact of the era of disruption and the influence of technology on the behavior of individuals and society highlights the need for continuous reformulation and updating of laws and regulations to ensure that they are relevant and effective in regulating behavior in the digital age. This requires a thorough review of existing legislation, as well as the development of new regulations, with special provisions or clauses that address issues related to technology, social media, and online transactions.

2. RESEARCH METHODS

Method was carried out in writing this journal was normative research, namely a process to find legal principles, legal principles, and legal doctrines to answer the legal problems faced (Marzuki, 2016) . In this study, the method used is a normative research that involves analysis of the principles of law and legal doctrine to answer the legal problems faced. The Data used in this study are in the form of library materials and secondary legal sources such as laws, regulations, Court decisions, and scientific papers. The analytical technique used is legal hermeneutics to obtain a clearer understanding of the legal material being discussed.

This research begins by formulating the problem to be studied, namely the impact of the era of disruption and the influence of technology on the behavior of individuals and society. Data is collected through literature study and search of legal sources relevant to the issue under study. Furthermore, the data is processed and analyzed using legal hermeneutics techniques to gain a deeper understanding of the legal materials used.

After analyzing the data, a discussion was conducted on the results obtained by linking the research findings with relevant legal concepts. The discussion discussed in detail the impact of the era of disruption and the influence of technology on the behavior of individuals and society as well as the legal implications arising from the situation Finally, conclusions are drawn based on the results of research and discussions that have been carried out. The conclusion summarizes the important findings of the study and provides recommendations for further action in overcoming the negative impact of the era of disruption and technological influence.

3. RESULTS AND DISCUSSION

3.1. Rationalization of criminology in the world of technology in a disruptive era.

Readers need to understand that 2023 is currently the year in which forms of communication that exist between individuals and groups with other groups tend to be larger by using increasingly advanced technology, namely the internet. One of the early forms that we understand in cyberspace is through international networks (internet); we can interact with anyone anytime, anywhere. Technology has transformed into a public space, as stated by Habermas. The internet is a public discussion medium that is open to everyone with various themes without any restrictions. Technology has also diverted human activities that were originally carried out in the real world—the presence of email, web blogs, chats and webcams on Facebook and Twitter.

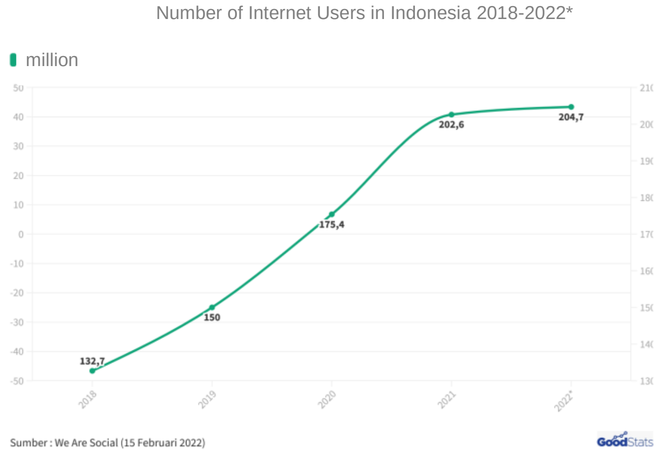
The above revolutionary changes in reality do not always have a positive impact, because the results of technological creations are known to always have two faces, that is, on the one hand they provide great benefits for human life, but on the other hand they also provide convenience and even expand criminal acts. global. Technological developments always have an impact, both directly and indirectly, both in a positive and negative sense and will greatly affect every attitude and mental attitude of every member of society. In terms of criminology, technology can be said to be a criminogenic factor, namely a factor that creates a person's desire to do evil or facilitates the occurrence of crime (Hamzah & Marsita, 1987). Departing from this, it is necessary to have a deeper understanding of the need for rationalization of criminology in technology in the current era of disruption.

There has been a change in people's understanding of technology in the form of rationalizations that they understand superficially regarding the use of technology; of course things that are considered normal and trivial will be done for the maximum benefit without regard to the regulations governing these matters as in Law no. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, which in this law has regulated various forms of violations that can occur in the world of technology today, down to the smallest matters, are regulated so that no detrimental to other technology users.

As stated in one of the articles, namely Article 30 paragraph (1) of the ITE Law, where every person intentionally and without rights or unlawfully accesses another person's computer and electronic system in any way. For the legal action of opening a cellphone without permission, the perpetrator who sees the contents of your cellphone without permission in any way and you don't want it will be punished with imprisonment for a maximum of 6 years and a fine of up to IDR 600 million. In another case, if the perpetrator looks into the contents of your cellphone to get your information and electronic documents, he is threatened with imprisonment for 7 years and a maximum fine of IDR 700 million. Meanwhile, suppose the perpetrator accesses the contents of your cellphone by violating, breaking through, bypassing, or breaking through the security system. In that case, you can be sentenced to a maximum of 8 years in prison and a maximum fine of IDR 800 million.

This was strengthened by the formation of additional regulations, namely Law no. 27 of 2022 concerning Protection of Personal Data, specifically Article 61 (1) Everyone who deliberately obtains or collects Personal Data that is not his own to benefit himself or others unlawfully or can cause harm to the Owner of Personal Data as referred to in Article 51 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years or a fine of up to Rp. 50,000,000,000.00 (fifty billion rupiah). (2) Any person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 51 paragraph (2) shall be subject to imprisonment for a maximum of 2 (two) years or a fine of up to Rp. 20,000,000,000.00 (twenty billion rupiah).

The two rules described by the author illustrate the efforts of the government to control the rate of development of the use of technology in the current era of disruption so as not to have a major negative impact on the wider community. However, the reality that is currently happening is the opposite, where many certain individuals deliberately commit acts that violate these rules for personal gain, such as using mobile phones (HP) that are already owned by all members of the public.


Number of Internet Users in Indonesia 2018-2022*

Sumber : We Are Social (15 Februari 2022)

Figure 1. Internet users in Indonesia

In early 2022 there were 204.7 internet users in Indonesia (*Examining the Development of Smartphone Use in Indonesia - GoodStats* , nd) of the total population of Indonesia in 2022 as a whole, there were 275,361,267 people as of June 2022 or semester I or around 89% of Indonesia's population had used cell phones. With so many people using mobile phones, it is easy for certain individuals to carry out criminal acts to seek profit (*What is Indonesia's Population in 2022? - National Tempo.Co* , nd)

The achievement of internet usage which almost touches 100% of Indonesia's current population, proves that technology is moving very fast so that it is known as the Disruption Era and it has a positive impact on the development of the Economy, Education to Law, however this impact also leads to things negative things, this is relevant to information. Based on data from ECPAT Indonesia, the consumption rate of pornographic content among Indonesians is alarming. From the results of a survey of adult video provider sites from America, Indonesia ranks second with the most access to porn videos.

This case looks just ordinary, the domino effect of this has a big impact, including many cases of rape and pregnancy out of wedlock, even from the latest data, from 2019 to the end of 2021 cases of early marriage in Indonesia have continued to increase according to data from the Ministry of PPPA and BKKBN, up 30 % every year. In Central Java alone in 2021 data by the Ministry of Religion of Central Java Province there were 8,700 cases of early marriage where when they wanted to carry out a marriage and get a marriage book they had to go through a trial or marriage dispensation case at the Religious Court. The increase in cases of early marriage occurred during the Covid-19 pandemic, and many women experienced marriage under the age of 19. Meanwhile, early marriage in Central Kalimantan (Central Kalimantan) is also still high. This data is based on BPS data for 2019, the marriage rate for women over the age of 10 years and over, including those aged 16 years (18.42%), aged 17-18 (22.55%), while those aged 19-20 (23.34%) , and age 21 (35.69%). Marriage at a young age is expected to continue to increase in the number during this corona pandemic. From 2021 to August 300 young children are married, in 2020 on the databoks.katadata.co.id website, Central Kalimantan ranks fifth after West Sulawesi.

The classification of crimes according to the theory of social criminology that is currently developing and adapted to the views of some criminologists is based on the existence of categories of crimes and some according to the process by which crimes occur, namely ways of committing crimes, techniques and organizations and groups that have value. - a certain value. The classes are as written by AS Nature. as follows: *Professional crime* , namely crime committed as a permanent source of income and having certain expertise for the profession, for example counterfeiting money, signatures, and pickpocketing. *Organized crime*, namely organized crime, such as extortion, trafficking in narcotics and illegal drugs. *Occasional crime*, i.e. crime by agreement, for example burglary in a shared home.

Of the three theories presented by the author, they are closely related to the use of current technology, for example the use of mobile phones. Starting from professional crimes, namely crimes committed as a steady source of income and having certain expertise for the profession, for example counterfeiting money, signatures, and pickpockets. With the current technology, Professional Crimes will certainly make adjustments. With this technology, it will be easier for professional criminals to adjust their knowledge because with the current technology everything is clearly and factually available; negative (wulandari, 2019).

Previously, cases of counterfeiting money or pickpocketing had to be carried out with extra effort and required a very large room, so it had to be carried out by more than one member, but in today's technological era, professional crime only requires a cellphone connected to the internet network, it will be very easy. to commit counterfeiting in cyberspace, especially with the existence of digital money that is developing at this time, as well as in cases of pickpocketing, you don't need to feel introspective if you are caught, you will be beaten up by a mob until you are seriously injured and even die. Simply by utilizing technology, blue-collar criminals sitting on cafe terraces can steal money from GoPay balances (electronic money) of people who are their targets.

Next is Organized Crime, which is organized crime, such as extortion, trafficking in narcotics and illegal drugs. Organized crime with existing technology will be able to actualize their knowledge of a wider range of crimes, namely:

a. Crimes committed by hacking or entering/infiltrating a computer network system unlawfully, or without permission or without the knowledge of the owner of the computer network system he entered. Usually criminals (hackers) do this with the intention of sabotaging or stealing important and confidential information (Sitohang & Fazrina, 2019) . However, there are also those who do it simply because they feel challenged to try their ability to penetrate systems that have a high level of protection. This crime is increasingly prevalent with the development of internet/intranet technology. Crimes committed with government objects with the motive of terrorizing, hijacking or undermining the security of a government with the aim of disrupting the government system, or destroying a country.

b. Crimes that enter network systems illegally or unauthorized access to computer systems and services are generally committed by hackers who deliberately abuse their skills to commit acts of theft. Many young Indonesian hackers who are students of IT systems admit that when they are caught, their criminal actions trigger their adrenaline and when they succeed, they are very satisfied, even having time to enjoy the proceeds of crime just for fun or pleasure. just have fun. causes of unauthorized access to computer systems & services Currently computer crimes are increasingly widespread, there are several things that cause more widespread computer crimes (unauthorized access), including:
   1) Unlimited internet access
   2) Negligence of computer users
   3) Easy to do and hard to track
   4) The perpetrators are generally people who have high intelligence and great curiosity. Weaker system security makes it easier for hackers/crackers to steal data. Many things can be done by a hacker / cracker to break into a system

c. Illegal content is a mode of cybercrime by entering data or information onto the internet about something that is untrue, unethical, and can be considered unlawful or disturbing public order. In its implementation, the illegal content that is currently developing is starting to take on a massive form and seem right, but in essence it is wrong (Nuriyah & Afifah, 2022) . An example is an advertisement for a product that depicts a brand ambassador like an artist to market its product. It looks like what the company hopes for so that its products sell well in the market with the logo "in seven days the skin color that was previously black can become pure white" but it turns out that what is depicted in the advertisement is not what consumers who see the advertisement expect, which only takes 7 the day their skin which used to be black became translucent white like the artist in the advertisement. Another example is that a consumer who eats or drinks is described when consuming it will make his body healthy within 10 days as explained by the company in a circulating advertisement, but in reality this is not true. In addition, the name of the intake used in the product mix uses English, so that people who do not understand English cannot see the ingredients of the food or drink ingredients that are traded which causes consumers or the public to consume them directly. This is a problem, because the advertisements described by the company do not match what is advertised. This is a form of massive content that is illegal because it depicts something that shouldn't be, as well as provides pseudo wishful thinking. This is a type of hidden fraud, in other words, it is structured illegal content

d. Data Falsification Is a mode of crime in cyberspace that is carried out by falsifying important document data stored as scripless documents via the internet (Sadino & Dewi, 2021) . This crime is usually aimed at e-commerce documents in a way as if there is a "typo" which will ultimately benefit the perpetrator, because the victim will enter personal data and credit card numbers that are allegedly misused by the perpetrator. One form of counterfeiting with today's technology is diploma forgery where the victim also needs the certificate for ceremonial purposes, while the perpetrator benefits from making a fake diploma so that no money is harmed, either the victim whose diploma is falsified or the perpetrator who forges his diploma. . How does the law see this problem and the system that can prevent this case. Clearer rules need to be made to ensnare perpetrators or victims.

e. *Cyber Espionage (Cyber Spionage)* Is a crime whose mode is to use the internet network to carry out espionage against other parties by entering the computer network system of the intended party. One well-known example of cyber espionage occurred in 2009. It was first reported by Google when the company noticed constant attacks on holders of certain Gmail accounts, which were later found to belong to human rights activists in China. After exposing the attack, 20 well-known companies, including Adobe and Yahoo, claimed to be affected by this espionage attack. Research from cybersecurity organization McAfee explains that "Aurora" is part of a file path on the attacker's machine that is included in two malware binaries associated with the attack. The main goal of this attack is to gain access to and modify the source code repository. According to the author, the analysis of this case can be seen from scientific criminology, which is rationalized based on current technology to be directed at criminal behavior, and starts from:

1) *Trace or* search – hackers are looking for systems that can be compromised. This activity includes determining the scope of attack and selecting and mapping networks.
2) *Scanning or* selection – hackers start looking for weaknesses in the system by targeting walls or easily penetrated gaps in the system.
3) Target data enumeration/search - the intruder will look for information about valid account names and existing shared resources. This stage has disrupted or disrupted the system.
4) *Gain access* – the hacker tries to gain access to the system as a normal user.
5) *Privilege escalation* – the hacker's stage of elevating a normal user to admin or root so that he can gain access to greater information.
6) Spying on data – cyber espionage starts with taking important information or data that is needed.
7) Create backdoors and delete traces - after acting, hackers will usually delete traces to minimize activity detection. Usually, hackers create backdoor or undocumented portals.
8) This polarization process is a study of criminology that is misused for negative things.

f. Sabotage and Cyber Extortion In this crime mode, it is usually carried out by disrupting, damaging or destroying data, computer programs or computer network systems connected to the internet. This crime is generally carried out by infiltrating logic bombs, computer viruses or certain programs so that data, computer programs or computer network systems cannot be used, do not function properly or work but have been controlled according to the wishes of the perpetrator, with remote cyber controlled by the perpetrator. . So that the victim inevitably has to follow the wishes requested by the perpetrator, namely by giving an amount of money with a nominal value that has been set by the perpetrator. In this case, we can judge that the current form of extortion is not only in the form of photos or videos of victims, but in the form of data on the internet, which can be manipulated to provide benefits for irresponsible parties. Another term is Ransomware, similar to the crime of extortion that we are used to, the pretext of using data from victims to gain profit by threatening to lock the victim's data if they do not make a ransom in the form of paying money.

g. Intellectual Property Violation This crime targets third party online intellectual property rights as its method of operation. For example, they illegally imitate the appearance of other people's websites. This problem is already very complex in the world of technology, including plagiarizing content on the internet, or what we know as copyright, is plagiarizing content on the internet, which can be in the form of text, images, videos, and so on. Generally this happens because of the ease of dissemination of information in cyberspace. This allows internet users to easily copy other people's content and recognize it as their own. Plagiarism like this is very prone to occur and is detrimental to the owner of the original content.

h. Another thing is Software Piracy. There are also cases of software piracy, where bad people will distribute certain software on the internet for users to get free of charge. In fact, to have it requires a license that must be purchased. Many users use pirated software because of the high price of original software, there are many pirated software such as Microsoft Office, Photoshop, Coreldraw, and others. Privacy Breach. These crimes usually target personal information stored in computerized individual data forms. If this information is known to other people, it can cause material and immaterial losses for victims, such as leaking of credit card numbers, ATM PINs, etc. This type of violation is usually disguised by several applications that the perpetrator intentionally sends to the victim, where by pressing the content sent, automatically all files on the victim's cellphone can be viewed and transferred to the perpetrator. So that without the victim's consent, their rights can be taken away by criminals using existing and increasingly sophisticated technology.

i. The last is occasional crimes, namely consensual crimes, for example burglary in the house together. Its implementation will be more structured and systematic based on existing technology and strengthened by misused scientific rationalization, especially in the study of victimology and criminology, because it is with this knowledge base that the perpetrators of Occasional crime. Not only stealing together in a house but also committing theft together in several big companies and even against the state. Corporate crime or corporate crime is a type of crime in which a company or corporation commits a crime. Corporate crime is included in white collar crime. Individuals or groups do so in their legitimate work to benefit the employing organization. Such people generally do not think of themselves as criminals or regard their activities as criminal acts. Examples of corporate crimes are business maladministration, neglect of EIA, bank fraud, sale of counterfeit securities, and patent infringement (Langton & Piquero, 2007).

The continuing development of science in the technological era in this disruptive era with universal and particular forms of rationalization. This raises the urgency to immediately carry out a comprehensive mapping of the social sciences, especially those studying criminology, which continue to experience significant developments in the era of disruption. The term in Dutch reads "achter de feiten aanlopen", which in English is translated as "behind the events", or in Indonesian means "behind the events/facts".

3.2. Law reform in preventing the formation of patterns of criminological rationalization in the world of technology in a disruptive era.

A real example is dispute resolution with the ODR (Online Dispute Resolution) option. Referring to existing regulations, laws and regulations in Indonesia have provided an alternative electronic transaction dispute resolution using this method. This is stated in Law Number 11 of 2008 concerning Information and Electronic Transactions and also in Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems (PP PMSE) (Rogers & Mohd, 1993) . Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions (ITE). It would be a breath of fresh air for technology security if the law was enacted in early 2000 when new technologies were being developed—considering that the ITE Law Number 19 of 2016, coupled with currently developing legal issues, is already very out of date with the adage " *behind the events /reality* ". So it's no wonder what is in the Constitution has not been able to trap the perpetrators of crime, especially in today's technological world. Although strengthened by Law no. 27 of 2022 concerning Protection of Personal Data (PDP), Law NO. 27 PDP does not cover all protections, especially in the realm of technology, especially in the internet environment that has protected almost all layers.

The several cases that the authors have described in the first problem formulation illustrate that the current Government Regulations have not been able to have an impact on the development of crime in the world of technology, especially in the current era of disruption considering that there are loopholes that can be exploited by irresponsible parties. responsibility to seek profit without violating the rules which are clearly stipulated in the laws and regulations made by the government. These irresponsible parties have even made several scientific breakthroughs by conducting studies with several experts to obtain patterns of crime that can ensnare as many victims as possible in the world of technology with the greatest possible benefits. Search can be compromised. This activity includes determining the scope of attack, selecting and mapping networks, and selecting targets and system weaknesses by aiming at walls or gaps that are easily penetrated in the system. Search data by target – intruders will look for information about valid accounts and shared resources. This stage is already disrupting the system. They were previously found in the data search stage until access to the system as a normal user. The last step is finishing in the form of cyber espionage, taking important information or data needed for their interests and eliminating traces so that they are not detected by the authorities, in this case Cyber Crime.

This proves that the current law requires comprehensive improvements to anticipate the polarization of criminology in technology in the era of disruption. This kind of problem cannot be underestimated by the government because this problem is like an "iceberg" phenomenon that only appears small on the surface, but the effect is enormous if we look inside. Problems that occur in society, especially with technology that continues to develop from time to time, make it necessary to conduct a thorough legal study, especially regarding legal sociology related to legal criminology, which examines the science that studies crime and criminal acts. The pattern of rationalization of criminology in today's technological world can be seen from several aspects of crimes that are increasingly structured and massive, including (Zakaria, 2022) :

a. Illegal access/Unauthorized Access to Computer Systems and Services (Unauthorized access to computer systems and services), is a form of crime committed by hacking or entering/infiltrating a computer network system illegally, or without permission or without the knowledge of the connected owner system computer network.

b. Illegal Content Is a mode of cybercrime by entering data or information into the internet about something that is untrue, unethical, and can be considered unlawful or disturbing public order.

c. Data Falsification Is a mode of crime in cyberspace that is carried out by falsifying important document data stored as scripless documents via the internet. This crime is usually aimed at e-commerce documents in a way as if there is a "typo" which will ultimately benefit the perpetrator, because the victim will enter personal data and credit card numbers that are allegedly misused by the perpetrator.

d. *Cyber Espionage (Cyber Spionage)* Is a crime whose mode is to use the internet network to carry out espionage activities against other parties by entering the computer network system of the intended party (Bendovschi, 2015)
e. Sabotage and Cyber Extortion In this crime mode, it is usually carried out by disrupting, damaging or destroying data, computer programs or computer network systems connected to the internet. Where usually this crime is committed by infiltrating logic bombs, computer viruses or certain programs, so that data, computer programs or computer network systems cannot be used, do not function properly or work but have been controlled according to the wishes of the perpetrator.
f. Intellectual Property Violation This crime targets third party online intellectual property rights as its method of operation. For example imitating the appearance of someone else's website illegally.
g. Privacy Breach. This type of crime usually targets personal information stored in computerized personal data forms. If this information is known to other people, it can cause material and immaterial losses for victims, such as leaking of credit card numbers, ATM PIN numbers, and so on(Martin, 2018).
h. *Runsomware* Similar to extortion crimes that we generally know, the pretext is to use data from victims to gain profit by threatening to lock the victim's data if they don't make a ransom in the form of paying money (Everett, 2016)

The patterns described by the author need to be seriously anticipated by the government by means of legal reformulation in preventing the formation of criminological rationalization in the world of technology in the era of disruption. Starting from the concept of hierarchy in laws and regulations departing from the theory of the legal system put forward by Hans Kelsen which states that the legal system is a system of steps with tiered rules. The relationship between the norms governing the actions of other norms and these other norms can be referred to as super and subordinate relations in a spatial context. The static norm system is a system that looks at the contents of the norm. According to the static norm system, general norms can be drawn into more specific norms, or special norms can be drawn from general norms (Baume, 2009). Meanwhile, a dynamic system of norms is a system of norms that views the validity of a norm from the way it is formed or abolished. Based on these two classifications of norms, in terms of knowledge of the legislation used is the second norm (Rodli, 2021). Therefore, it becomes an urgency in itself to carry out the reconstruction of the legal order in the world of technology and which, according to the author's analysis, can be started from:

a. The existence of legal certainty arises from the basic idea of the need for legal norms in every legal product that is born. As Hans Kelsen said, law is a system of norms. Norms are statements that emphasize the "should" or das sollen aspects, by including some rules about what must be done. These rules then become guidelines for individuals to behave in society, both in relationships with fellow individuals and in relationships with groups. These rules also become a limitation for society in burdening or taking action against individuals so as to give birth to legal certainty (Marzuki & Sh, 2021) .
b. The characteristics of information technology which are continuously developing and progressing, it can be predicted that in the future something similar will occur. If at this time there has been significant progress in the field of technology, especially related to electronic transactions compared to the previous few years, it can be projected that similar things will occur, namely more advanced developments in the next few years. Assafa Endeshaw looks at this problem, he argues that the legal positioning behind the development of information technology does not necessarily justify the absence of long-term thinking in drafting legal arrangements. He emphasizes that even though technology is developing so quickly and it is difficult to predict (Endeshaw et al., 2007) .

c. The effectiveness of law is often trapped in a subjective point of view. This is because there are many parameters that must be met to measure whether a law that is implemented into laws and regulations has worked well and has had a good impact so that it can be said to be something useful.

d. The regulation of electronic transaction laws still seems gray in Indonesia. In terms of drafting regulations and law enforcement, both indicate that there are rules that have not been implemented effectively and maximally.

e. The complexity of regulations regarding electronic transactions is a fundamental problem of the difficulty of technology law. Aspects that are so broad and intersect with various lines of life make information technology, especially electronic transactions, a party that works to formulate regulations because it can cause harmonization problems with other laws and regulations. The rapid development of technology has an impact on innovations in the form of activities related to electronic transactions which further complicate the code because it can lead to potential legal conflicts, legal ambiguity and even legal uncertainty. Departing from these problems, the option of the omnibus law legal model can be one of the solutions that are currently relevant. Omnibus law can be used as a tool that can help unravel the problems of technological law regulations which are so complex and intersect with other fields. This is because the omnibus law can quickly, effectively and efficiently resolve legal conflicts and limitations as well as standardize statutory policies that have been made to minimize the occurrence of legal disputes.

4. CONCLUSION

Current technological developments can be easily applied by all levels of society, so that by itself the spread of this knowledge can be absorbed and studied by all levels of society so that there are opportunities for some individuals to do negative things in the current technological era. So that by itself legal problems do not decrease but instead continue to increase. The mushrooming of legal problems in the world of technology today needs to be anticipated by the government so that by carrying out legal reformulations to prevent the formation of patterns of criminological rationalization in the world of technology in the era of disruption. By way of making regulations that are more specific by taking into account the principles of certainty, expediency and fairness. With clear and special and complex characteristics and regulations.

REFERENCES

Alam, A. S., & SH, M. (2018). *Kriminologi Suatu Pengantar: Edisi Pertama*. Prenada Media.

Baume, S. (2009). On political theology: A controversy between Hans Kelsen and Carl Schmitt. *History of European Ideas*, *35*(3), 369–381. https://doi.org/10.1016/j.histeuroideas.2009.01.001

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Berapa Jumlah Penduduk Indonesia Tahun 2022? - Nasional Tempo.co. (n.d.). Retrieved January 28, 2023, from https://nasional.tempo.co/read/1671308/berapa-jumlah-penduduk-indonesia-tahun-2022

Cerita di Balik Konten Mandi Lumpur TikTok, Nenek Sari Rela Tahan Dingin Berjam-jam demi Dapat Cuan Jutaan Rupiah Halaman all—Kompas.com. (n.d.). Retrieved January 28, 2023, from https://regional.kompas.com/read/2023/01/22/151856178/cerita-di-balik-konten-mandi-lumpur-tiktok-nenek-sari-rela-tahan-dingin?page=all

Cushman, F. (2020). Rationalization is rational. *Behavioral and Brain Sciences*, *43*, e28. https://doi.org/10.1017/S0140525X19001730

Dotsika, F., & Watkins, A. (2017). Identifying potentially disruptive trends by means of keyword network analysis. *Technological Forecasting and Social Change*, *119*, 114–127.

Endeshaw, A., Purwandari, S., Hananto, M. W., Waluyati, & Barkatullah, A. H. (2007). *Hukum e-commerce dan internet: Dengan fokus di Asia Pasifik*. Bina Ilmu.

Esturgo-Deu, M. E., & Sala-Roca, J. (2010). Disruptive behaviour of students in primary education and emotional intelligence. *Teaching and Teacher Education*, *26*(4), 830–837.

Everett, C. (2016). Ransomware: To pay or not to pay? *Computer Fraud & Security*, *2016*(4), 8–12. https://doi.org/10.1016/S1361-3723(16)30036-7

Hamzah, A., & Marsita, B. D. (1987). *Aspek-aspek pidana dibidang komputer*. Sinar Grafika.

Hasil Pencarian—KBBI Daring. (n.d.). Retrieved January 28, 2023, from https://kbbi.kemdikbud.go.id/entri/rasionalisasi

Kurniawan, S. (2019). Tantangan Abad 21 bagi Madrasah di Indonesia. *Intizar*, *25*(1), 55–68.

Langton, L., & Piquero, N. L. (2007). Can general strain theory explain white-collar crime? A preliminary investigation of the relationship between strain and select white-collar offenses. *Journal of Criminal Justice*, *35*(1), 1–15. https://doi.org/10.1016/j.jcrimjus.2006.11.011

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, *82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Marzuki, P. M. (2016). *Penelitian Hukum, Edisi Revisi, Cetakan Ke-12*. Kencana.

Marzuki, P. M., & Sh, M. S. (2021). *Pengantar ilmu hukum*. Prenada Media.

Mengulik Perkembangan Penggunaan Smartphone di Indonesia—GoodStats. (n.d.). Retrieved January 28, 2023, from https://goodstats.id/article/mengulik-perkembangan-penggunaan-smartphone-di-indonesia-sT2LA

Nuriyah, S., & Afifah, W. (2022). ANALISIS KASUS PEMERASAN AKIBAT PENYALAHGUNAAN PADA SOSIAL MEDIA. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *2*(3), 1241–1251.

Rahmadsyah, R., Saktisahadan, T. J., Widodo, B., Abrarsyah, A., & Fadli, F. (2021). SOSIALISASI PEMANFAATAN TEKNOLOGI DI SEGALA SEKTOR PADA BIDANG TEKNIK MESIN DI DESA BAGAN ASAHAN PEKAN KECAMATAN TANJUNG BALAI KABUPATEN ASAHAN. *RAMBATE*, *1*(1), 21–26.

Rastati, R. (2016). *Bentuk perundungan siber di media sosial dan pencegahannya bagi korban dan pelaku*. Bandung Institute of Technology.

Rifauddin, M., & Halida, A. N. (2018). Waspada cybercrime dan informasi hoax pada media sosial facebook. *Khizanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *6*(2), 98–111.

Rodli, A. (2021). Rekonstruksi Pengaturan Hukum Transaksi Elektronik Di Indonesia. *Lex Renaissance*, *6*(2), 280–297.

Rogers, E. M., & Mohd, Z. (1993). *Teknologi komunikasi: Media baru dalam masyarakat*. Dewan Bahasa dan Pustaka.

Sadino, S., & Dewi, L. K. (2021). Internet Crime Dalam Perdagangan Elektronik. *Jurnal Magister Ilmu Hukum*, *1*(2), 9–17.

Sitohang, J. J., & Fazrina, B. B. (2019). TINJAUAN KRIMINOLOGI MEMASUKI ATAU MENYUSUP KEDALAM SUATU JARINGAN KOMPUTER SECARA TIDAK SAH MENURUT UU NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Ilmu Hukum Prima (IHP)*, *2*(1), 126–139.

Subasman, I. (2019). *Peran evaluasi pendidikan pada era disrupsi*.

Sururiyah, L. (2017). Tinjauan Kriminologi terhadap Suami Pelaku Penganiayaan dalam Rumah Tangga. *De Lega Lata: Jurnal Ilmu Hukum*, *2*(2), 328–350.

Utomo, S. (2017). Tantangan Hukum Modern Di Era Digital. *Jurnal Hukum Media Bhakti*.

Wibawa, I. (2016). Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme). *Masalah-Masalah Hukum*, *45*(4), 285–291.

WULANDARI, J. T. R. (2019). *TINJAUAN KRIMINOLOGIS TERHADAP TINDAK PIDANA PENIPUAN DENGAN CARA PENYADAPAN APLIKASI WHATSAPP (Studi Kasus Kota Makassar 2017-2018)* [PhD Thesis]. Universitas Hasanuddin.

Zakaria, H. (2022). *ETIKA PROFESI DI BIDANG TEKNOLOGI INFORMASI*. Pascal Books.