

Exploration of AI Victimization in Everyday Practice through the Lens of Structuration and Legal Policy Challenges

Ferlansius Pangalila

Department of Criminology, Faculty of Social Science and Political Science, University of Indonesia, Indonesia

Received 23-04-2024

Revised 24-04-2024

Accepted 09-05-2024

Published 11-05-2024



Copyright: ©2024 The Authors. Published by Publisher. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

Abstract

AI plays a role in social change this is due to factors that influence social interaction through various AI models as a means of connecting users with AI structures in the practice of daily social life. This research aims to understand AI victimization through the lens of structuration theory in the daily life practices of individuals and society, by exploring the experiences of victims and the factors that influence AI victimization. The findings show that there are various forms of AI victimization in the relationship between victims and the AI structure due to the presence of endogenous and exogenous factors in people's daily activities. The implication of this research is the importance of more effective legal policies in social protection, especially for victims of AI victimization.

Keywords: AI Victimization, Endogenous Factors, Exogenous Factors, Structuration Theory, Legal Policy

Introduction

Implementation and use of AI technology in society in this era has made a huge contribution to the transformation of various aspects of social life. AI is present and applied in various arenas of social life such as health (Freeman et al., 2017), education (Merchant et al., 2014), entertainment (Lin, Wu, & Tao 2018) and various other aspects of life (Bonetti, Warnaby, & Quinn, 2018). Social interactions in various aspects of social life have formed new realities related to AI. From the perspective of AI space and time, this does not only happen in the physical world or the virtual world but can happen back and forth (vice versa) and even mixed (exponential).

However, various challenges and risks also arise, including AI victimization. This may be

because the AI structure through various existing AI models still has various algorithmic shortcomings, such as training data that was obtained unethically or still has the potential for bias in its implementation. At the level of use, there are various situational compulsions and system obligations as structural obstacles that have the potential for victimization. Therefore, there is a need to understand AI victimization, not only as a technological phenomenon in the era of industrial revolution 4.0, but also as a complex social and legal problem. Through the lens of structuration, experiences and perceptions of victims, this research analyzes in more depth the dynamics of social interaction, namely the relationship between individuals and social structures through the means between various AI models in daily practice.

Even though many experts have researched the impact of AI technology ambivalence in the form of studies of the pros and cons of AI technology, and several criminologists have researched and linked this to cybercrime (Caldwell et al., 2020; Hayward & Maas 2021; King et al., 2020), understanding of AI victimization in the context of victimology is still limited. In fact, there is still little attention to the relationship patterns of individual actions and AI structures in the occurrence of victimization as well as exploring the factors that influence this through victim experience and expert opinion, such as public policies that give rise to situational compulsions, algorithmic system obligations that impact constraints and limitations in use that have the potential for victimization systematic and symbolic victimization, including considering some criminal behavior related to AI. Thus, through this research, we gain a more holistic understanding of the dynamics of AI victimization and encourage the development of legal policies that are more effective in protecting and serving victims from various potentially detrimental AI victimizations.

The aim of this research is to understand in depth the victims' experiences and perceptions of AI victimization, as well as the role of these factors in influencing their perceptions of AI victimization. Through structured interviews and a structuration theory approach, this research will identify patterns, themes and structures that emerge in the responses of key informants, as well as explore the relationship between victims and AI structures related to exogenous and endogenous factors that influence victims' attitudes and perceptions resulting in victimization AI. Thus, this research aims to gain a deeper understanding of the dynamics of AI victimization, and contribute to the development of public policies that are more effective in overcoming the challenges of implementing and utilizing AI in everyday practice.

The conceptual framework in this research is based on first, AI victimization, which refers to various forms of loss and negative impacts experienced by victims in relation to the AI

structure through means between various AI models. Second, Anthony Giddens' structuration theory, which highlights the importance of the relationship between agency and social structure which is dual in nature, as social interactions produce and reproduce social structures, which in turn shape human interactions and subjective experiences. By utilizing these two concepts, this research will explore the complexities of AI victimization in various arenas of everyday social practice.

This research has significance in the context of sustainable social change in this era. By better understanding various AI victimizations and the various factors that influence them, we can develop social protection strategies, especially for people who use various AI technologies through legal policies. In addition, this research can contribute to the development of theory and methodology in the field of victimology and AI technology.

Structuration Theory Lens:

In Giddens' structuration theory, the relationship between AI and social structure is to understand the concept of mutual interaction between agents (individuals or groups as users of AI technology) and social structures. In this structuration theory, access and control over technology is part of the social structure that is formed through social interaction, this influences the distribution of power and its influence on society. Therefore, AI can be seen as a social structure because it represents patterns that are implemented in systems programmed by humans (in its development there are several systems that are programmed by AI technology without any further human involvement) and enforced in social life (Figure 1). AI itself is regulated by norms, policies and various rules set by the government, companies or the industrial world itself, and on the other hand is determined by the practical actions of society in its use (structural duality).

When we talk about the structure of AI, we are talking about various scheme-like rules related to AI technology, namely automation, digitalization, instrumentalization, and

personalization with various schemata related to AI and the consequences of its ambivalence. The structure of AI when linked to structuration theory will be very helpful in understanding the complexity of interactions

between humans and AI, how individual (human) actions shape and influence the structure of AI technology, and how the structure of AI influences individual actions and behavior.

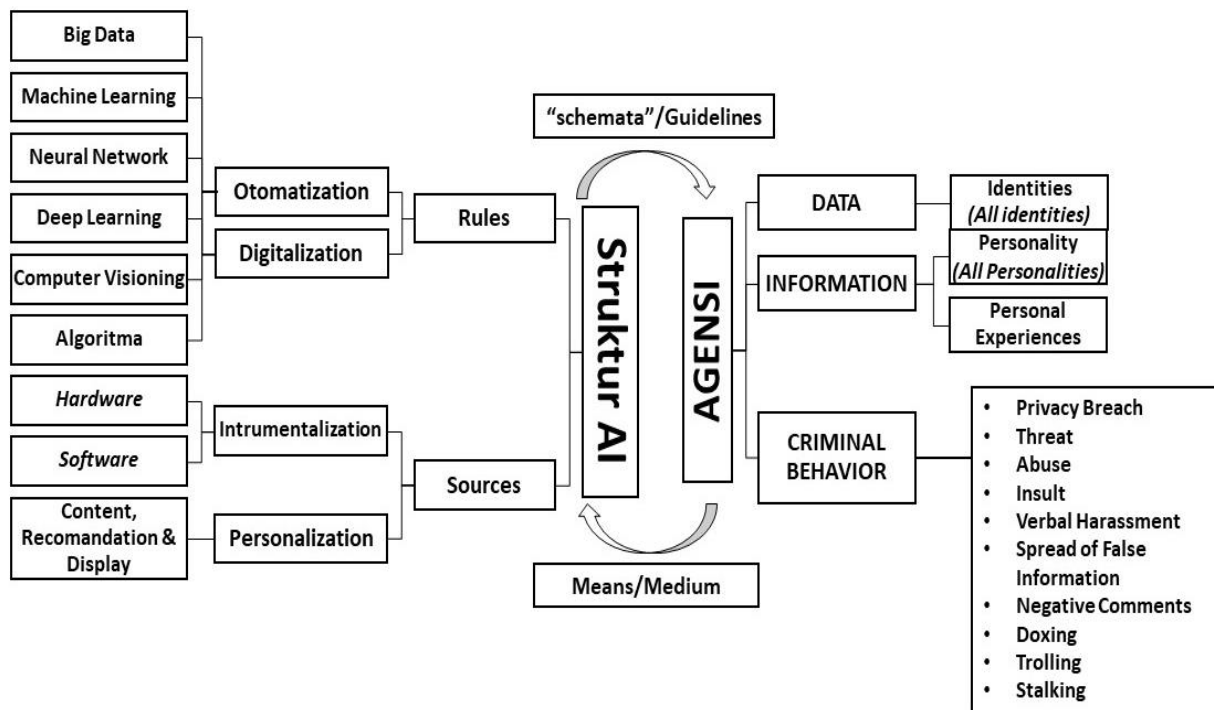


Figure 1. Pattern of Relationship between AI Structure and Agency

AI structure can refer to both the architecture of artificial intelligence, including the AI models, algorithms and infrastructure that make up that artificial intelligence for the purpose of making decisions or providing services. Meanwhile agency refers to the role and actions of humans as users in interacting with various AI models that exist in daily life practices such as accessing, interacting and/or responding with and/or through these various AI models. It is called agency because users have the role and ability to interact, control, utilize and or even exploit AI according to their intentions, interests and/or the actions they choose.

Agencies or users have autonomy because they are able to understand the direction of their actions, their impact on other users and in what context the actions are carried out. When this autonomy is lost or reduced, users have the potential to become victims regarding the implementation and use of this AI technology. This relationship pattern in the context of AI

victimization includes repeated dynamics and interactions between AI structures and agencies (users) which give rise to impacts such as exploitation and abuse, dependency and others that are present in social practices because these interactions have become routines carried out by individuals in their lives his daily life.

AI victimization can mean three things, namely victimization by AI, victimization with AI and victimization in AI. These three things have different meanings but are interrelated or not separate, therefore researchers combine these three things with the term AI Victimization (AIV), which in this research can refer to one or all three of these meanings at once.

Research conducted by Hallevy shows that several (Bayern, 2015; Hallevy, 2015) AI models have similarities with legal entities/corporations, therefore AI can be considered an entity that can be held legally responsible, at least as Bavaria believes that there needs to be regulation in the

form of a law that regulates legal responsibility for artificial intelligence entities by legal entities jointly or severally.

Victimization by AI refers to situations where an AI model is the perpetrator of a negative or detrimental impact whether intentional or not. Some examples that occur are errors in decision making by AI models in employee recruitment which has been researched by several experts as often experiencing bias. Other potential threats such as cyber-attacks that work automatically. In business practices other than the examples above, it can be found how pricing algorithms often occur automatically on various e-commerce platforms, where the sale of counterfeit goods and/or unfair pricing can occur. Victimization by AI is possible because of the structure of AI automation, namely the AI model can carry out performance tests on it self and develop new skills, and can process millions of data or commands in a short time and continuously without stopping.

With the implementation and use of AI in everyday social interactions, it is possible for anyone to commit crimes by utilizing this technology. Research conducted by Brundage et al (Brundage et al., 2018) shows that AI technology can be used as a tool in committing crimes, there was a case in Spain in 2022, where a Drone (unmanned aircraft) operating under water transporting drugs to be smuggled through the Strait of Gibraltar. Another example is cyber-attacks carried out by humans by utilizing AI as a tool in carrying out attacks to increase the effectiveness and impact of attacks, such as in cyber cases terrorism.

Victimization with AI is commonly used by criminals because of the anonymity structures that are possible in some AI technologies, where perpetrators can carry out criminal behavior without their identity being known to the victim or authorities. In many cases, this anonymous structure is widely used by perpetrators to reduce the risk of being discovered or avoid responsibility and is used as an alibi even though these various criminal behaviors result in victims or victimization (Figure 2).

Victimization in AI or through AI is the most common in daily social life practices (Hallevy, 2015). Where the use of various AI models is often unethical or aims to harm other people. Examples include fraud that uses algorithms or cyber-attacks to identify security gaps and launch detrimental attacks, many cases relate to this in everyday life.

In interactions with social media, victimization through AI is most often found in behavior that, whether consciously or not, has resulted in victims. Sharing false information or hoaxes is often found in social media practices, the use of deepfake technology which is deceptive which of course can harm a person's reputation or integrity (Marshall, Lefringhausen, & Ferenczi, 2015; Suraya & Kadju, 2019; Zhou & Makse, 2019). In a political campaign atmosphere, it is often a buzzer used to spread false messages to attract support or harm an opponent's reputation (Suraya & Kadju, 2019; Zhou & Makse, 2019) and this can also trigger social conflict.

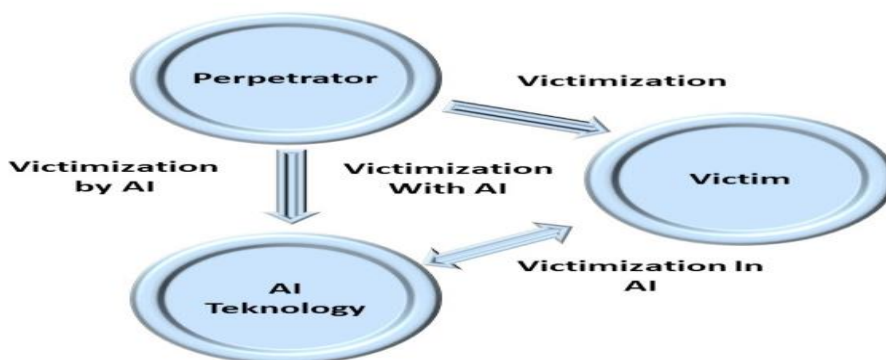


Figure 2. Relationship between Perpetrators, Victims and AI Technology

Body Text

Researchers conducted an analysis of victimization that occurs in everyday life related to the implementation and use of AI technology in daily life practices, so that researchers can identify various forms of AI victimization from various data that researchers found both from primary data and secondary data in the field direct. This research uses a qualitative approach with unstructured interviews. This approach was chosen because it provides depth of understanding of individual experiences and allows for in-depth exploration of the dynamics of AI victimization in everyday social practices. A variety of experiences from key informants were selected to deepen understanding of the perceptions and experiences of AI victims in specific situations and arenas.

Key informants who are classified as AI victims will be selected through criteria that include individuals who have experienced or been affected by AI victimization in various arenas, namely in the arenas of social, business and criminal (cybercrime) practice, as well as in political practice. The selection of informants in these various arenas is to ensure diversity in experiences and various perspectives regarding AI victimization which is caused by the connection between the AI structure and the victim's actions in space and time as the arena.

The data collection process will be carried out face to face with informants who have been selected and are willing to be interviewed. Interviews will be recorded with the informant's permission and then transcribed accurately for further analysis; some informants ask not to be recorded but may note important points for later analysis. During the interview, informants will be given the opportunity to express their experiences freely, while maintaining the confidentiality of their identities.

Interview data will be analyzed using a structuration approach. This analysis will include identifying patterns, themes, and structures that emerge in the informants' responses, as well as how both endogenous and exogenous factors influence

their perceptions of AI victimization. This analysis will be carried out using an inductive approach to enable the discovery of new and in-depth findings.

Results and Discussions:

Results:

The data obtained in this research shows that AI victimization occurs due to the existence of a pattern of reciprocal relationships (linkages) between the AI structure and agency (individual) actions in the dimensions of space and time as the AI horizon. AIV lies in the interrelationships that occur in daily life practices that continue to repeat themselves (recursion). Informants stated that in their connection with the AI structure in social practice through sharing AI models as an intermediate means in daily social interaction, they experienced various forms of AI victimization, including: Addiction and vulnerability through social media, online games and online gambling, vulnerability in lending practices online, vulnerabilities in online transportation practices and online shopping. Apart from that, informants also experienced various forms of victimization in criminal practices such as online fraud, identity theft and fake pornographic content.

Further analysis revealed a complex relationship between user reflexivity that emerged in interviews and structural factors influencing respondents' perceptions of AI victimization. Factors such as public policies that do not pay attention to the basic rights and interests of victims, system obligations and symbolic restrictions by AI corporations in the implementation and use of various AI models in daily practice, in addition to corporate practices that prioritize profits over empathy and compensation for victims, as well as criminal behavior of other users in utilizing various AI systems such as misuse of privacy data and personal characteristics of victims. Therefore, the next challenge is to develop legal policies as a form of social protection as well as efforts to prevent and minimize AI victimization in daily life practices.

Discussion:

AI applications and services in daily routines has influenced the social structure, where debates

regarding the social impact of various AI technology products continue to emerge (Joyce et al., 2021). A characteristic of the Industrial Revolution era is the development of AI technology (Baldwin, 2016; Schwab, 2016), where this technology has a very significant impact on the social structure of society. AI technology has influenced various aspects of social life including social interaction, communication, societal organization, and the distribution of power (Elliott, 2019). The way of communicating in this era has changed significantly to become easier, faster, and more efficient with the existence of social media, instant messaging, and smartphones. Communication thus influences the way people interact, share information, and build social relationships (Korenich et al., 2013).

Technological developments such as social media have brought about changes in the way social organizations act in society (Korenich et al., 2013). People can easily find and form virtual organizations online based on certain shared interests or hobbies with the help of the internet and various digital platforms. Organizations that were previously physical have now entered the virtual world and, in its people, can organize their activities, share information, and even gather support and mobilize it (Plant, 2004; Preece, Maloney-Krichmar, & Abras, 2003). In the world of work, AI technology with online collaboration has helped many jobs that previously had to be done physically in the office or company, but now many jobs can be done remotely work (Flores, 2019).

This provides the context that AI technology can be viewed as a “Structure” that influences individual actions and social structures (de Rafael & Fernández-Prados, 2019). On the one hand, AI technology itself is as a limiting structure or shape human actions through algorithms, artificial intelligence, and the rules contained therein. Various AI platforms and applications influence individuals or groups to act in decision making by influencing, limiting, or even directing the available options.

Victimization is the process of creating victims, of course what is emphasized is the process of creating victims, in addition to the elements of perpetrator and victim being an inseparable part of victimization theory itself. Therefore, it is necessary to see AI victimization as a process of causing victims due to the reciprocal relationship between the AI structure and agency (human actions) which continues to be repeated as a practice of daily life in the space and time dimensions of the AI horizon, including the factors drivers of AI victimization.

Of the 212.9 million internet users, 167 million people are active social media users. Until January 2023, as can be seen in graph 5.1, this figure is equivalent to 60.4% of Indonesia's population (APJII, 2023). Social media is the AI structure most often used by people daily for social interaction or just relaxing. In carrying out activities related to AI, users often obtain various information whether desired or not and share the information they obtain via social media with other users, including misinformation in the form of hoaxes. Users are often attacked with various advertisements for goods and services, and most of them are goods or services that the user has been looking for or wants (advertising targeted).

AIV in Social Practice:

Several key informants experienced dependence or even addiction to high-tech and up-to-date smartphones. Every time there is a new smartphone product with higher specifications, the informant will try to buy it, even if it is on credit through various online financing applications. Buying a sophisticated smartphone is not only for work effectiveness but more for following an existing lifestyle. The informant felt very happy if he could have a smartphone from a well-known brand with the latest specifications. If he succeeds in buying it, the informant will usually show it off on social media so that his family and friends know that he was able to get it.

This dependency behavior is driven by endogenous factors, namely the informant's hedonism to become consumptive and wasteful so

he is willing to buy a smartphone even though the price is high. AIV in the context of dependency and vulnerability occurs due to the relationship between the AI structure and the victim's actions which influence each other so that victimization occurs. In showing this, the informant acted because he was driven by endogenous factors, such as self-esteem and narcissism and driven by exogenous factors with the involvement of existing AI structures that enable these actions to occur in various applications and services such as personalized AI structures in the form of psychological manipulation through advertising targeted, where users of various social media are deceived by consumer goods advertised based on personal data and characteristics.

The fact is that social media has become a new mode of social interaction in this era, where almost all forms of social interaction are through and facilitated by AI structures in various social media platforms such as Facebook, Instagram, Twitter and TikTok and others with their respective advantages and benefits. The data found shows that this social media provides joy, passion, and convenience for its users. In several previous studies such as those conducted by, we are social and meltwalter with his report in July 2023 as many as 4.88 billion social media user identities with an average of more than 2 hours spent every day.

Several informants revealed that in their daily lives they are very dependent on various AI technology-based devices and applications, such as virtual assistants and automation systems. In the world of work, AI really helps in completing daily work. Even though the informant realized that due to frequent use of AI, the informant felt less productive and not independent in carrying out tasks manually. It seems that the informant's analytical ability is reduced because his "brain" has not been sharpened and used for a long time like before the AI structure in the AI systems and applications currently used. This dependence also carries over to activities at home and in the social environment. The informant experienced dependence without realizing it, this was because

the AI structure in the various models used by him every day was very easy for the user to operate even though the user had no basic knowledge of technology.

Several informants who work as housewives depend on several AI based applications specifically for social media and e-commerce. AI has caused an addiction to continuously use various AI devices and applications in everyday life in terms of convenient shopping through various e-commerce applications, spending time every day searching various items that are desired in the application, and every time the informant finds the desired item, the informant puts it in the shopping basket then looks for similar items and continues to put them in the shopping basket repeatedly. This routine is often carried out by informants for hours and continues to be repeated every day.

Informants said that most of these items were not purchased, but only because they felt happy and experienced psychological satisfaction when seeing various advertisements offered by the application. Enjoying seeing advertisements and reading reviews from previous buyers made the informant become dependent or addicted and continues to do so to this day. Apart from dependence on various e-commerce applications, informants also experience dependence on various social media applications. Informants will spend hours just scrolling through various digital applications without realizing it, they have spent productive time, mostly watching various broadcasts and short videos on social media applications, reading and commenting on statuses or just by liking various interesting photos and videos. Even though it was only short videos (reels), commenting on statuses or even clicking on various symbols in the social media application, several informants admitted that they had wasted more than two hours of productive time every morning and evening (an average of more than four hours a day), often doing activities I still do this regularly before going to bed at night.

Several informants who were previously social media users chose not to use it anymore

because they considered social media to be poison that had succeeded in destroying creativity, time and relationships between themselves and other people, especially their families. Previously, the informant felt tied to social media and experienced an addiction. The informant uses social media to send various creative results such as his writing or whatever he considers to be his life achievements.

However, these informants felt that what they did via social media was considered by their family, colleagues, and some social media friends to be the informant's attempt to brag about themselves (flexing). The informant admitted that he really hoped to be praised by his family, colleagues, and friends on social media for what he posted because for him what he posted was an achievement worth being proud of. However, apart from praise, informants felt that they were often not appreciated or even ignored by their families or even co-workers just because their posts were not responded to or commented on by their families and co-workers.

The informant's feeling of being unappreciated gradually turned into a feeling of dislike which he expressed by never wanting to comment on or even liking uploads sent by his family and co-workers, even though he always saw them on his social media home page. Informants often feel ignored or disliked by their social media friends simply because they do not react by liking or commenting on their uploads through various symbols provided by various social media applications (passive symbolic victimization). Finally, the informant's disappointment culminated in him deleting all his social media accounts.

This is different from several informants who still use social media but are passive. Like an informant who, although he rarely comments on and/or ticks' symbols of liking or disliking his friends' uploads, informants often feel uncomfortable with other people's uploads and think that their uploads are hoaxes, flexing or make the informant feel that their life is not as lucky as theirs. For example, some of the informant's friends often post on social media eating at luxury

restaurants, showing off new cars, traveling to tourist attractions or showing off their beauty and/or other advantages, which for the informant is luck that only they can enjoy and is misfortune. for those who can't experience that. The informant continues to experience feelings of envy and misfortune towards his family and friends on social media which he often views every day. This causes the informant to become asocial on social media (not commenting or not checking like/dislike symbols but always feeling jealous and cursing himself).

Some informants often have a negative attitude towards their friends' posts with sneers or insults which cause discomfort to the person who sends something on social media by providing signs or symbols (active symbolic victimization). Friendship on social media has a different meaning from friends in the non-digital world, it may be that friendship on social media consists of people who know each other or are just followers or fans (who are also not fans in the true sense). Friends, Followers or Fans are more interpreted as accounts that are accepted and given access to be able to see each other and comment or react to the uploads of the received account. Including access that could cause related accounts or people to experience victimization.

As experienced by an informant who received a vacation award from his workplace as a reward for achieving work targets. Traveling to the European continent made the informant like a celebrity in his company. Making him the center of attention of his co-workers who did not get the holiday, therefore, a few moments after the informant was announced as the recipient of the bonus, online stalking occurred, where the informant's social media account provided notifications of friendships by many new accounts previously not friends with him. Most of his friendship accounts on social media are people he knows as family or work colleagues; old friends and the rest are some he does not know at all.

During his tour, the informant often sent photos of his activities via social media because he

felt proud and happy while at these tourist attractions, however, his activities on social media by sending several uploads caused the informant to experience victimization. Several of his social media friends commented negatively on his post and thought that the informant was just an employee who received a travel bonus in an inappropriate way (active symbolic victimization). Friends' comments on social media regarding several of his posts on social media caused the informant to become frustrated and damaged his own mental state so that when he returned to the office the informant felt uncomfortable working with his colleagues who he considered to be a group of criminals who had hurt him in cyberspace, not for long then the informant chose to leave the company.

What was experienced by the main informant above shows that social media not only causes addiction but can also create vulnerability as a victim, where AI victimization can occur due to social interactions in various social media applications allowing someone to feel uncomfortable and even lose their job. Apart from that, the AI structure in social media makes it possible to group people into hate groups and together they can do what is called cancel culture. AIV which often occurs due to flexing activities on social media and can develop into cancelation culture for various groups of people. According to Koentjoro, that Cancel culture the same as a boycott, where a public figure or person with influence can suddenly be cancelled or rejected because they are deemed no longer in line with the wishes of the community, via social media or by submitting a petition.

AIV in Criminal Practice:

AIV is the interrelationship between the AI structure and the agency's actions in the dimensions of space and time causing victimization. This refers to the pattern of relationships between AI structures and human actions that may be due to the personal actions of the person concerned or other parties who carry out certain actions, thereby causing victimization. One of the causes of AI victimization

is criminal practices by users of various AI models against other users, resulting in victims.

AI structures and human actions in social interactions has resulted in various AI structures continuing to be created with the need in various applications to include personal data such as NIK, email address, number. Mobile phones and in fact almost all existing applications require the user to agree that the application can access the user's smartphone with permission to access all contacts, photos, and videos as well as all existing documents. If this access permission is not granted, it is certain that the application in question cannot be utilized or used. The problem is, some victims often receive telephone calls and/or receive short messages from various parties, from legal insurance companies whose corporate names are quite familiar to various completely unknown parties offering certain products or services and/or receiving calls like what was experienced by several informants in online loan cases.

One of the informants shared his experience of experiencing online fraud through an online shopping application that he often uses every day. What he experienced was a phishing case, where the perpetrator created a website which is very similar to the website original company, the method is to send a message via social interaction media on a smartphone, that the informant gets a shopping discount of 90% on the goods he wants which is often seen from one of the e-commerce (the perpetrator can track, find out and analyze the victim's behavior and character through various AI applications on the victim's smartphone).

Informants are asked to go to the website linked in the message and follow the next steps. After opening the website in question, the informant enters several important data such as name and address, then via message the informant receives an OTP number (one time password) and enter it on the website the. Informants are informed that the OTP sent is confirmation of the correctness of the address and willingness to pay for the discounted goods. Because informants feel confident with advertisements and websites. The

company looks genuine, the informant follows all the instructions in question.

However, after following the instructions in the form of a chatbot suddenly the application used by the informant to communicate with the chatbot is out and cannot be used again for a while. At that time, the informant realized that his smartphone had been hacked through the application and immediately received an SMS notification that there has been a debit to his bank account for the total amount of his money in the bank. The informant immediately panicked and immediately called the bank in question and asked to block his account. However, his efforts were in vain because all his savings had been drained and transferred to the fraudster's account.

Another informant also experienced the same story. Initially this informant received an e-mail from one of the banks of which he is a customer of that bank. The informant received an attractive offer, namely an "interbank transfer" transaction which was not charged with an administration fee for each transaction even though the transaction was carried out many times by the informant. Informants only need to agree by opening the e-mail attachment and following the next instructions. The informant downloaded the e-mail attachment and follow the instructions provided. Without realizing it, the informant had been deceived and as a result lost quite a large amount of money in the bank account. The informant immediately acted and contacted her husband to go together to the relevant bank and ask to return the transaction money because it turned out to be a fraud. This was revealed because the bank never had or was currently running the free interbank transfer transaction fee program referred to by the fraudster.

The fraud experienced by the informant turned out to result in other victimization, where when the informant and her husband reported the case, it turned out that the service to the victim by the Bank was very unpleasant and the problem was not resolved either. The bank asked the informant and her husband to make a police report first and

on that basis the bank could take further action such as withholding the money. However, when they returned to the bank after making a police report which took hours, the informant was only told by the bank that the money had been transferred to another bank account by the perpetrator and the bank could not do anything more.

In several cases experienced by informants in criminal practices related to AI technology, it shows that AI victimization has occurred in everyday life, as was also conveyed by one of the victims who experienced AI victimization in terms of creating fake pornographic content, in where the perpetrator utilized a deepfake AI application to carry out threats, fraud and other crimes. As experienced by one of the informants. It started with the informant frequently sending selfies on social media, but what he sent on social media was still within reasonable limits and never in the context of pornography. But what he experienced was very embarrassing for him. One day he received a WhatsApp message from an unknown number, and when he opened the message, it turned out to contain naked photos with a face that was very similar to his own.

It can be confirmed that the face is hers but the naked body in the photo is not hers. Therefore, the informant immediately deleted it and ignored the message. However, a few days later the photos were sent again with several pornographic videos in which the face in the video was very similar to the informant's real face. The message was accompanied by a threat that the photos and videos would be distributed by the perpetrator if the informant did not respond to the message. Because he felt embarrassed and afraid, the informant answered the message, asking who and what his intention was to send him such photos and videos. The perpetrator answered that it was an original video of himself and would be distributed by the perpetrator on the campus where the informant studied. Because he felt that the photos and videos were fake, the informant did not respond.

The next day, one of his good friends called to say that he had received a naked photo of the informant with a threat from the sender that the photo would be distributed everywhere if the informant did not respond to his request. The informant knew that it was fake, while if other people saw it, they would think it was genuine and indeed to the naked eye it looked very similar or genuine because of the sophistication of AI technology. Finally, the informant contacted the perpetrator and asked what should be done so that the fake photos and videos were not circulated elsewhere. The informant was asked by the perpetrator to send a certain amount of money to the account sent by him and the informant was not allowed to tell this to anyone, if he told it, the photos and videos would be distributed.

Legal Policy Challenges:

This research also found that there is a need for legal policies related to AI in various sectors of social life to balance the development and use of AI technology with the current massive victimization of AI. So, on this occasion a legal conception is needed as a legitimating structure for various forms of AI victimization. In the legal conception of AI, there are at least two main problems in the legal system in Indonesia, namely:

- 1) Urgency of Legal Policy regarding AI;
- 2) Criminal Policy (Criminal Policy) Regarding AI.

AI technology has changed social life (Harari 2015, 2018; Schwab, 2016), and this change is happening very quickly along with the presence of various AI models in social life itself (Abbas and Rasool, 2021), at least various AI models, both in the form of smart devices and AI-based applications and services, have become a means and consumption of everyday society day. Of course, as explained above, the impact of ambivalence and the use of AI in everyday life has the potential to lead to AI victimization, which has encouraged the government to continue to strive to minimize its negative impacts, among other things, through various policies and legal regulations.

In the future, the singularity of AI and artificial superintelligence will increasingly be realized (Eden, 2016; Krüger, 2021; Walsh, 2020), one day AI will develop far beyond human intelligence and change civilization and humanity, where AI with superhuman intelligence can continue to increase its intelligence beyond human intelligence, some experts even say it will happen starting in 2030. Of course, this has the potential to be a victimization of AI which will become a serious problem in the future, at least now it has caused concern for many people, especially not a few who question the development and application of this AI technology in the practice of everyday life, as stated by Stephen Hawking and Elon Musk, that one day AI will be a disaster for humanity (Corrales, Fenwick, and Forgó, 2018).

The development and implementation of AI technology as well as social reactions to the application of AI technology in social practice in the form of pros and cons or social analysis of the various ambivalent impacts of AI technology are the basis for determining and regulating matters related to AI victimization. This effort is a criminal policy in reconstructing criminal law in the form of statutory regulations related to AI.

Several countries have attempted to create policies both in the form of statutory regulations and in the form of policies in the form of ethical standards related to innovation in the development and public use of AI technology (Table 1). At the global level, the United Nations Educational, Scientific, and Cultural Organization (UNESCO) has published Recommendations on the Ethics of AI (UNESCO, 2021), which was later adopted by 193 member states as an AI Ethics framework. Of the several countries that have adopted UNESCO's recommendations, there are two policy models taken by these countries, whether they choose one or both, namely: first, making special Legislation regarding AI, or second, making guidelines in the form of Ethical Standards regarding AI.

Table 1. Some Countries with AI Policies

No.	Country	AI Policy
1	United States of America	There are several laws at the federal level related to AI and are regulated in certain sectors, namely: finance, health and transportation
2	European Union	- UNESCO's Ethical Guidelines for AI, - Constitution AI that aims to provide clear requirements and obligations to developers and their implementation
3	Canada	Several federal and provincial regulations relate to AI, especially in the context of privacy and data protection.
4	China	There are national policies that encourage the development and adoption of AI, but there are no specific laws that explicitly regulate the use and development of AI.
5	Japan	Adopt AI-related policies and guidelines, with a focus on innovation and ethics
6	South Korea	There are several laws and regulations related to the development and use of AI, especially in the context of information and communication technology
7	Singapore	Issued several guidelines and regulations related to AI, especially in technology regulations and data privacy

The legal concept regarding the victimization of AI in the form of legal policy has become urgent because in social, business, and political practices related to the implementation and use of AI, it has caused victims, even though in many cases the victims are not aware of it. Most AI does not pose a significant risk of victimization, but the potential for AI victimization will become increasingly massive and more dangerous with its very rapid development. Therefore, there is a need for laws that regulate AI.

Various legal policies always contain values, concepts, and objectives such as those contained in the European Union's AI law which has the following objectives:

- 1) addressing risks specifically posed by AI applications;
- 2) prohibit AI practices that pose unacceptable risks;
- 3) define a list of high-risk applications;
- 4) establish clear requirements for AI systems for high-risk applications;
- 5) establishing specific obligations for parties implementing and providing high-risk AI applications;
- 6) require conformity assessments before certain AI systems are used or marketed;
- 7) implementing law enforcement after certain AI systems are marketed.

AIV which has anomalous and exponential characteristics, is a challenge in building legal conceptions regarding AI, especially in determining appropriate legal policies related to the application and use of various AI models in social life practices. Researchers see various complexities that will be faced in carrying out legal conceptions and statutory regulations related to AI, namely as follows:

- 1) Efforts to resolve AI's status as a medium or tool used in committing crimes or violations mean that AI is only an object (intermediate means) and/or AI as an actor or legal subject (source).
- 2) Sectoral efforts, namely separating AI-related issues into legal provisions in each sector or field, for example AI related issues in health law, education and various legal regulations in other social practices;
- 3) Conception efforts relate to the main material in criminal law, namely determining criminal acts or deeds, criminal liability and punishment or criminal sanctions. This relates to what actions or actions can be categorized as criminal acts related to AI, who can be charged with criminal responsibility, and the type of punishment imposed.
- 4) Non-penal efforts against various AI-related actions that have the potential to victimize AI, because criminal resolution should be the last resort in resolving AI-related problems (ultimum remedium).
- 5) Technical policy efforts, this is related to the creation of fundamental new legal norms, and as an effort to change these new legal norms in text form into legal norms in the form of algorithmic code so that they can be implemented into various AI models as a form of protection and prevention of AI victimization.

Conclusions and recommendations:

AI in various AI models is in the form of hardware, software and brain-ware not only as a tool produced to make work easier or just a luxury

entertainment item, but with the AI structure in the form of automation, digitalization, instrumentalization and personalization it has changed the way of life and even humans themselves, influencing humans more in making important decisions in life and having an impact ambivalence includes victimization, in addition to that technological singularity is increasingly becoming a reality with a more dangerous level of risk, with an exponential scale of development. Therefore, the urgency to carry out supervision and action is needed through regulations and appropriate ethical standards and legitimacy.

Criminal policy is the path that must be taken by the government in dealing with the development and use of AI in social practice. Criminal policy related to AI is an issue that is not easy to see AI as a legal object. The problems associated with AI are very complex and related to many factors, so when carrying out criminalization it is very necessary to take this complexity into account. Starting from what types of acts can be criminalized, of course not only acts that are essentially evil in nature, but also neutral acts that do not seem to be essentially evil but these acts have the potential to be detrimental both materially and psychologically.

Suggestions and Future Research:

This research provides valuable direction for further development in the field of victimology and the study of the use of AI in social life. In conducting future research, it is necessary to expand the scope of informants in various areas of life related to the use of AI. The large number of informants from various backgrounds and contexts can provide a more comprehensive picture of the relationship patterns between AI structures and users so that AI victimization occurs along with the factors that influence it.

Research using a qualitative approach with a quantitative approach could be a productive step to deepen understanding of AI victimization with better analysis of the findings. In addition, further research could also explore certain aspects of AI victimization that have not been revealed in this research, such as its impact on vulnerable groups or

its implications in legal and public policy contexts. As such, these suggestions provide valuable directions for continued research aimed at developing our understanding of the complexity of the AI victimization phenomenon in late modern societies, as well as providing a stronger foundation for the development of more effective response strategies and policies in the future.

At the policy level, various legal aspects such as legal principles and ethical studies need to be researched further, because AI technology is exactly like the law itself which in the context of the AI structure can be guidelines, rules and even the algorithm itself which has great potential in creating social reality and social engineering. This further research is very necessary to help the authorities in making legal policies related to AI in the future. The legal debate regarding criminal liability by AI is still ongoing in the academic world to this day, of course this opens up opportunities for victimologists to offer various ethical standards in the legal conception of AI, especially in victim services and mitigation which already needs to be done, because even though policies and regulations are not yet adequate. Currently, AI in various models has been implemented and used daily.

References:

1. Abbas, M. & Rasool, G. (2021). Artificial Intelligence in Our Daily Life. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 7(1), 417-421. <https://doi.org/10.48175/568>
2. APJII. (2023). *Internet Penetration & Behavior Survey 2023*. Jakarta.
3. Baldwin, R. (2016). *The Great Convergence; Information Technology and the New Globalization*. The Belknap Press Of Harvard University Press.
4. Bayern, S. 2015. The Implications of Modern Business-Entity Law for the Regulations of Autonomous Systems. *Stanford Technology Law Review*, 19(93), 93–112.
5. Bonetti, F., Warnaby, G., & Quinn, L. (2018). *Augmented Reality and Virtual Reality in Physical and Online Retailing: A Review, Synthesis and Research Agenda in Augmented Reality and Virtual Reality*. Springer, Cham. pp. 119–132.
6. Brundage, M., Avin, S., Clark, J., Toner H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S. O., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crotoft, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*.
7. Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-Enabled Future Crime. *Crime Science*. 9(1), 14. <https://doi.org/10.1186/s40163-020-00123-8>
8. Corrales, M., Fenwick, M., & Forgó, N. (2018). *Robotics, AI and the Future of Law*. Singapore: Springer Nature Singapore Pte Ltd.
9. Eden, A. H. (2016). *The Singularity Controversy, Part I: Lessons Learned and Open Questions: Conclusions from the Battle on the Legitimacy of the Debate*.
10. Ar Xiv, 1601, 05977. <https://doi.org/10.13140/RG.2.1.3416.6809>
11. Elliott, A. (2019). *The Culture of AI: Everyday Life and the Digital Revolution*. New York: Routledge.
12. Flores, M. F. (2019). Understanding the Challenges of Remote Working and Its Impact to Workers. *International Journal of Business Marketing and Management (IJBMM)*, 4(11), 40–44.
13. Freeman, D., Reeve, S., Robinson, A., Ehlers, A., Clark, D., Spanlang, B., & Slater M. (2017). Virtual Reality in the Assessment, Understanding, and Treatment of Mental Health Disorders. *Psychological Medicine*, 47(14), 2393–2400. <https://doi.org/10.1017/S003329171700040X>

14. Hallevy, G. (2015). *Liabilities for Crimes Involving Artificial Intelligence Systems*. New York: Springer.
15. Harari, Y. N. (2018). *21 Lessons for the 21st Century*. London: Jonathan Cape.
16. Hayward, K. J. & Maas, M. M. (2021). Artificial Intelligence and Crime: A Primer for Criminologists. *Crime, Media, Culture*, 17(2), 209–33. <https://doi.org/10.1177/1741659020917434>
17. Joyce, K., Smith-Doerr, L., Alegria, S., Bell, S., Cruz, T., Hoffman, S. G., Noble, S. U., & Shestakofsky, B. (2021). Toward a Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change. *Socius*, 7. <https://doi.org/10.1177/2378023121999581>
18. King, T. C., Aggarwal, N., Taddeo, M., & Floridi L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, 26(1), 89–120. <https://doi.org/10.1007/s11948-018-00081-0>
19. Korenich, L., Lascu, D., Manrai, L., & Manrai, A. (2013). *Social Media: Past, Present, and Future*. Routledge Companion to the Future of Marketing. 234-249.
20. Kruger, O. (2021). The Singularity Is Near! Visions of Artificial Intelligence in Posthumanism and Transhumanism. *International Journal of Interactive Multimedia and Artificial Intelligence*, 7(1), 16–23. <https://doi.org/10.9781/ijimai.2021.07.004>
21. Lin, J. H. T., Wu, D. Y., & Tao, C. C. (2018). So Scary, yet so Fun: The Role of Self-Efficacy in Enjoyment of a Virtual Reality Horror Games. *New Media and Society*, 20(9), 3223–42. <https://doi.org/10.1177/1461444817744850>
22. Marshall, T. C., Lefringhausen, K., & Ferenczi, N. (2015). The Big Five, Self-Esteem, and Narcissism as Predictor of the Topics People Write about in Facebook Status Updates. *Personality and Individual Differences*, 85, 35–40. <https://doi.org/10.1016/j.paid.2015.04.039>
23. Merchant, Z., Goetz, E. T., Cifuentes, L., Kennicutt, W. K., & Davis, T. J. (2014). Effectiveness of Virtual Reality-Based Instructions on Students' Learning Outcomes in K-12 and Higher Education: A Meta-Analysis. *Computers and Education*, 70, 29–40. <https://doi.org/10.1016/j.compedu.2013.07.033>
24. Plant, R. (2004). Online Communities. *Technology in Society*, 26(1), 51–65. <https://doi.org/10.1016/j.techsoc.2003.10.005>
25. Preece, J., Maloney-Krichmar, D., & Abras, C. (2003). History of Online Communities. In *Encyclopedia of Community: From Village to Virtual World*, edited by K. Christensen and D. Levinson. Thousand Oaks: Sage Publications, 1023–27.
26. Rafael, G. H. & Fernández-Prados, J. S. (2019). Victimization, Social Structure and Psychosocial Variables: The Case of Spain in 1999 and 2016. *Social Sciences*, 8(3), 102. <https://doi.org/10.3390/socsci8030102>
27. Schwab, K. (2016). *The Fourth Industrial Revolution*. Switzerland: World Economic Forum.
28. Suraya, S. & Kadju, F E. D. (2019). Jokowi versus Prabowo Presidential Race for 2019 General Election on Twitter. *Saudi Journal of Humanities and Social Sciences*, 4(3), 198-212. <https://doi.org/10.21276/sjhss.2019.4.3.6>
29. UNESCO. (2021). *Recommendations on the Ethics of Artificial Intelligence*. UNESCO.
30. Walsh, T. (2020). The Singularity May Never Be Near. *European Union's Horizon*.
31. Zhou, Z. & Makse, H. A. (2019). Artificial Intelligence for Elections: The Case of 2019 Argentina Primary and Presidential Election. *ArXiv*. 1910, 11227. <https://doi.org/10.48550/arXiv.1910.11227>