Electronic Journal of Education, Social Economics and Technology
Vol. 6, No. 2, (2025), pp. 1-9, Article ID: 282
ISSN 2723-6250 (online)
DOI: https://doi.org/10.33122/ejeset.v6i2.282

SAINTIS publishing

Research Article

Urgency of Ai Verification Rules to Enforce the Validity of Information on the Deepfake Phenomenon: A Comparative Study of Indonesian Positive Law and the Blueprints for an Ai Bill of Rights of the United States

Hanuun Zainum A*, Laina Rafianti

Faculty of Law, Universitas Padjadjaran, Kampus Unpad Jatinangor, Jl. Ir. Soekarno KM. 21, Jatinangor, Sumedang, Jawa Barat, Indonesia
*Corresponding Author: hanuun20001@mail.unpad.ac.id

ABSTRACT

Artificial intelligence technology, also known as human AI, is becoming more common and developing as human civilization becomes more modern. AI is not only known as humanoid robots; AI has also developed into software, computer systems, and programs. One of the AI innovations that has attracted attention is deepfake. The development of image and video manipulation technology has had serious consequences for the integrity of information and the reputation of agencies and individuals. This AI technology can easily cause disinformation. It is very easy to use this technology to spread misleading information, influence public opinion, and even trigger civil unrest. Furthermore, the author will compare Indonesian positive law and the Blueprints for an AI Bill of Rights as a guideline for United States AI to be able to minimize deepfake against disinformation. Legislation and conceptual theory are the main approaches used in the juridical-normative legal research method.

Keywords: Artificial Intelligence; Deepfake; AI Guidelines

1. INTRODUCTION

In line with the advancement of science, technological development is necessary as part of a country's development process. In the digital era, humans must utilize easy access to information and communication technology that supports their daily lives to continue creating a more advanced society. The overall lifestyle of modern humans is inseparable from electronic gadgets. In practice, theories and principles are often not in line with the reality on the ground and will always go hand in hand with unexpected possibilities. In the digital era, this poses new challenges for technology in human life.

The development of artificial intelligence (AI) technology innovation is synonymous with Industrial Revolution 4.0 and Industrial Revolution 5.0. There is no denying that AI significantly impacts people's daily lives. The concept of the 5.0 era was first adopted by Japan in the *Basic Policy on Economic and Fiscal Management and Reform 2016* through the *5th Science and Technology Basic Plan,* aspiring to create a society where everyone can live a better life. Therefore, integrating the virtual and real worlds to develop data, information, and a higher quality of life is key to achieving this goal. In fact, according to the *International Telecommunication Union* (ITU), the UN body involved in telecommunications, artificial intelligence will impact most of our lives in the future (Ramli, 2024c).

Artificial intelligence is defined by the *World Intellectual Property Organisation* (WIPO, 2016) as the creation of computer-based technologies and systems capable of performing tasks that require human intelligence through machine learning and deep learning. Thus, technologies that enable machines to act intelligently like humans are what we call artificial intelligence.

The ability of robotic machines to learn from experience and perform activities associated with human intellectual abilities, including language comprehension, logic, and problem-solving, is known as artificial intelligence. This is inseparable from the impact of digital transformation as a consequence of technology that causes artificial intelligence to continue to develop and become more sophisticated (Kristophorus Hadiono, 2020). At the same time, the results of artificial intelligence cause the *output of* obscurity and are difficult to accept by Indonesian law because its existence is not supported by apparent legal certainty (Rizki Fauzi, Tasya Safiranita Ramli, 2022).

Artificial Intelligence-Crime (hereinafter abbreviated as AIC) is a term for artificial intelligence misused by cybercriminals. The *deepfake* phenomenon or *audio/video impersonation* is one example of AIC in today's technological

advancement. *Deepfake* technology has caused potential chaos in cyberspace and the real world. The term "*deepfake*" refers to an algorithm that allows users to mimic real-world visual objects by transforming one person's face into another. This technique can be applied to both photos and videos. *Deepfake* is an artificial intelligence-based method or approach to creating synthetic human images (Ellen Kusuma and Nenden Sekar Arum, 2022). Furthermore, the process behind *deepfake* involves two main methods, namely:

a. *Deep Neural Networks* (DNN):

   With DNN, *deepfake* production using machine learning technology can blend a person's face into another video. Collecting the source video and target face data is the first step in this procedure. Deep learning methods train a network model to perfectly mimic eye, lip, and facial movements through extensive literacy and training. After training, the model can realistically *input* facial data into other videos (Sari, 2024a).

b. *Generative Adversarial Networks* (GANs):

   Discriminators and generators are the building blocks of GAN. The discriminator learns to distinguish between real and fake data, and the generator generates new data closer to the accurate data. GAN builds a model that can develop material that looks or sounds like it was produced by someone else using actual video or audio as training data. This creates an environment that favors spreading false information and possible harassment, which can harm society (Sari, 2024b).

The first use of *deepfakes* was in 2017, and it became more serious after the launch of the *FakeApp* app in 2018, which allows users to edit and swap faces between people with video output. Unfortunately, the negative impact of *deepfakes* is alarming. According to data from *Home Security Heroes*, 95,820 *deepfake* videos were distributed worldwide in 2023. Digitally altering sounds, images, and videos to portray a message that never happened in reality can be done with *deepfake* techniques (Patria, 2024).

The development of digital technologies, especially in image and video manipulation, has seriously affected the integrity of information and the reputation of bodies and individuals. It is easy for these technologies to spread misleading information, influence public opinion, and even spark civil unrest. Unlike humans, technology has no boundaries against which to act and make decisions. Despite its extraordinary ability to process data or recognize complex patterns, AI cannot determine whether information is against ethical, moral, or legal norms. Vulnerability to misuse of algorithms can potentially lead to disinformation (PLEADS FH Unpad, 2024).

In connection with the threat of *deepfakes* regarding information, in October 2023, a video of President Joko Widodo giving a speech in fluent Mandarin language went viral on various media platforms. Shortly after the content appeared, the Director General of Applications of the Ministry of Communication and Information Technology (hereinafter Kemenkominfo), Samuel Abrijani, immediately confirmed that the video was a misleading edit (Mediana, 2023). Further ahead of the election, *deepfakes* became a "big concern," as Prime Minister (PM) Narendra Modi said of the election in India. Micro-targeting of disinformation and spreading false narratives can influence voting behavior (Welle, 2024). The presence of *deepfakes* has led to confusion and difficulty in distinguishing between valid information and fake news. While there have been no reports of substantial material losses due to *deepfakes*, the fact that this technology exists raises concerns about potential future impacts. The Ministry of Communication and Informatics has responded by appealing to the public to be more aware of *deepfakes* that can cause disinformation. It has also urged the public to proactively anticipate *deepfake* cases that may arise (Sari, 2024b).

Law enforcement's validity depends solely on where the criminal offense was committed, and that place must be within the territory of the state concerned. In cybercrime, jurisdiction is crucial. A state gains full recognition and sovereignty over its laws and policies when there is jurisdictional certainty. Concerning traditional jurisdictional principles relating to the limits of state authority in three areas of law enforcement, referring to Masaki Hamano's opinion entitled "Comparative Study of Jurisdictional Approaches in Cyberspace" (Galih, 2019), are as follows:

1. *Jurisdiction to prescribe.* The ability of a state to enact laws appropriate to its society and current circumstances is known as legislative jurisdiction. Regarding the internet, the question arises as to which state has jurisdiction over individuals or actions in cyberspace. This raises an issue, namely "*choice of law*".
2. *Jurisdiction to adjudicate* is the state's power over individuals to conduct court hearings in criminal cases. In this case, the issue is "*choice of forum*."
3. *Jurisdiction to enforce*, relating to the authority of a state to punish the defendant according to the applicable law, either through the courts or through other non-legal actions (administrative sanctions).

Masaki Hamano distinguishes between a legal perspective and a cyber/virtual perspective on cyber jurisdiction. "The authority of system operators and users to make rules and enforce them in society in cyberspace/virtual space" is a standard definition of cyber jurisdiction from a cyber perspective. Legally, *cyber* jurisdiction, also known as a jurisdiction in *cyberspace*, refers to the actual *physical* control of governments and courts over internet users and their online behavior

(*physical government's power and court's authority over net users or their activity in cyberspace*).

Countries like the United States, the European Union, China, and Brazil have made various arrangements. On 11 May 2024, the Council of Europe stated in its official statement on the EU AI *Act* under *Blueprints for an AI Bill of Rights* that this regulation is an essential legal norm in this era that was previously unknown. As a global norm, the EU AI Act will serve as a regulatory framework for countries outside the EU. There will be a transition period before the law comes into effect. The EU AI Bill of Rights will promote AI regulation that provides a controlled setting for the creation, evaluation, and verification of new AI systems and the practical testing of AI advances (Ramli, 2024a).

As the *Blueprints for an AI Bill of Rights* is not a binding document, it will not be independently enacted for administrative purposes, as mentioned the document shares with a more specifically American law the EU AI *Act*. The process of creating this document, which began in 2021, aims to declare a world charter of rights with respect to AI. This right is a step in the right direction which will then take the form of regulating the use of AI more specifically (Floridi, 2023).

Meanwhile, in Indonesia, the publication of the National Strategy for Artificial Intelligence 2020-2045 document became the initial reference for the development and utilization of artificial intelligence in Indonesia. Stranas is currently in the process of becoming a draft presidential regulation (Heriani, 2024). However, as AI is a new technology, there is currently no official regulation governing it. Although the Ministry of Communication and Information in Indonesia has issued ethical guidelines for AI, the recommendations are only basic principles without specific policies. Given that Indonesians are already making extensive use of AI technologies, particularly in digital platforms, social media, commercial operations, government, and the use of chatbots, the country should thoroughly evaluate AI laws and develop a regulatory framework (Ramli, 2024b).

Quoting the theory initiated by Mochtar Kusumaatmadja, it is said that "law as a tool of social engineering", the law should not be anti-change and should not support the *status quo*. Law must be nurtured and developed so as to provide space for development. That is, the law must "appear at the forefront and show the direction of development" (Mochtar Kusumaatmadja, Otje Salman, 2002) in creating a good social-technological climate. Furthermore, through statutory instruments, the plan for change and development is set as a guide for the community and government when going through the process of change and development so that the community and government arrive in an orderly and peaceful manner at the destination of change and development as aspired (Imamulhadi, 2017).

According to Ahmad Ramli's theory of transformation law, the role of law is not just as a development institution, but also as a transformation infrastructure that needs to go hand in hand with public policy (Ahmad Ramli and Tasya Safiranita, 2022). The law should be the basis for taking an action. According to Ahmad M. Ramli's transformative legal theory, the legal system as a whole must be able to collaborate and react quickly to technological advances. Therefore, the current Indonesian legal system is not affected by the rapid advancement of technology. Given, in the theory of *lex digitalis* it can also be understood that there is no one virtual space that is not a legal jurisdiction (Maudy Andreana Lestari, Ahmad M Ramli, 2022).

In this regard, to prevent possible AI offences, today's rapid technological advances must be supported by appropriate regulations (Ahmad Ramli and Tasya Safiranita, 2022). Therefore, the presence of regulations is important to adjust to the current state of technology (Feliany Kowanda, Miranda Risang Ayu Palar, 2024). One of the important roles of regulation is to provide guidance on how AI can be addressed. In the event of a violation, the use of AI will be able to go hand in hand with regulation and law enforcement. Thus, to protect human rights and promote an enabling environment for AI technology, regulators play an important role.

2. RESEARCH METHOD

The author uses a normative juridical research method. Normative juridical analysis involves the use of secondary data or library sources to examine laws and regulations and connect them with legal events that occur in society. This research uses research specifications, namely descriptive-analytical, which includes explanations in looking at descriptions and images regarding applicable laws and regulations and legal conditions in a particular location.

In this research, the author will compare the US AI guidelines or *Blueprints for an AI Bill of Rights* in the United States as a comparison and hopefully can be a reference for future Indonesian law. The reason for choosing the US as a comparison is because the US as one of the leading countries in AI development has more comprehensive legal tools as one of the leaders of the technology industry and the first originator of AI regulations. Regarding the digital sovereignty paradigm, US practices and regulations are interesting to study because they are well documented. The US initially implemented a policy of non-regulation and non-intervention, but over time the US began to implement written regulations related to its policies, especially related to the internet (Ramli, 2024a).

The following will explain several reasons for the urgency of the research raised by the author, among others: First, the need for legal certainty guaranteed by the legislator that is methodically applied by certain authorities is the juridical reason for the need for a special law governing AI. Second, legal certainty that provides protection for the parties is a sociological reason. Third, in order to grow the country's economy, the philosophical reason is to provide security and

stability to the parties. Fourth, adding practical reasons, the existence of a special law governing AI will allow society to adjust to all types of AI-related activities (Santoso, 2018). The purpose of this research is to analyse the extent of legal protection provided by Indonesia and the United States as a comparative study in providing protection against disinformation, and to see what forms of preventive rules can be applied in Indonesia to minimise disinformation in the digital era.

3. RESULTS AND DISCUSSION

3.1 Legal Arrangement of *Artificial Intelligence* in Indonesia and Its Problems

Artificial Intelligence (AI) is being used as research to study how computers can do things that can now be done more effectively by humans. The ability to reason and act in the method most likely to achieve a goal is one of the characteristics of AI. The main purpose of AI is to facilitate reasoning, learning, and other processes. With the advent of this technology, it will become increasingly difficult for people to identify or detect the authenticity of altered photos or videos as AI becomes more complex. With respect to photo or video content distributed online, inappropriate use of *deepfake* technology can be considered a cybercrime.

Currently, the regulation of artificial intelligence or AI in Indonesia can refer to the provisions of Law Number 1 Year 2024 on the second amendment to Law Number 11 Year 2008 on Electronic Information and Transactions (hereinafter referred to as ITE Law) as *Lex Generalis*. A device in an electronic system that is made to automatically perform an action on certain Electronic Information performed by a person is the definition of "Electronic Agent". Thus, the automation of AI information processing can be considered as an "Electronic Agent", which is in accordance with the definition of electronic agent itself stipulated in Article 1 paragraph (8) of the ITE Law.

In the fragment of the Article, "automatic" refers to independent operation. Furthermore, the definition of artificial intelligence technology is a computer-based processing system capable of independent thinking and decision-making. Therefore, the characteristics of the "Electronic Agent" itself can be compared to the characteristics of artificial intelligence/AI technology (Priowirjanto, 2022).

AI actually falls under the definition of Electronic Agent, which means that all legal obligations and legal responsibilities are imposed on the provider of the Artificial Intelligence device (Priancha, 2024). This is emphasised in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (hereinafter referred to as PP PSTE), which defines an Electronic Agent as a device that aims to perform an action in the form of electronic information automatically arranged by an individual or corporation and is part of an electronic system (Article 1 Point 3, PP PSTE, 2019).

The phrase "organised" indicates that there is an electronic system controller as the Electronic Agent, thus, there is a legal relationship between the Electronic System Controller (PSE) and the Electronic Agent User, where AI acts as an Electronic Agent which is part of the PSE itself. In this regard, it is explicitly regulated that the self-organisation of electronic systems can be carried out by electronic system controllers or through Electronic Agents (Article 36 paragraph (1), PP PSTE, 2019).

Deepfake as a misuse of AI is categorised as a prohibited act when referring to the ITE Law, which states that actions without rights and intentionally carried out by people in order to show, broadcast, and make accessible electronic documents and electronic information for public knowledge and the content is a violation of decency (Article 27 paragraph (1), ITE Law).

Furthermore, the threat of imprisonment for a maximum of 6 years and/or a maximum fine of Rp1 billion can be applied to parties who violate the provisions of Article 27 paragraph (1) of the ITE Law. However, the exemption from punishment applies in the event that it is carried out for self-defence; public welfare; or is of an artistic, cultural, sporting, health, and/or scientific nature represented in electronic information and/or documents (Article 45 paragraph (1), ITE Law, 2024).

Furthermore, referring to Article 21 of the ITE Law, to organise an electronic system, parties such as the state, individuals, legal entities, and communities must have the status of legal subjects. On the other hand, AI is an open-source platform that is not managed by a specific legal institution. Unlike other online marketplaces such as Bukalapak or Tokopedia, which are companies that build technology systems, this is different. The difference is that *open-source* AI is not a company or person in charge of the business division that plans the electronic system. This leads to the consequence that the legal liability of AI will only be borne by the controller of the electronic system that organises AI services. Thus, the current regulation is still very broad and not very specific because it is limited to referring to the ITE Law as *Lex Generalis*.

This leads us to conclude that while still general in nature, existing laws already refer to technology in the form of artificial intelligence (AI) as "Electronic Agents." Internet abuse that disturbs public or private order may be punishable under the relevant laws or regulations, depending on the specific circumstances. Regrettably, however, the current law does not touch upon the follow-up of the execution of the "Electronic Agent" itself. Regulations regarding security measures against the presence of AI are also not mentioned in this law. Thus, issues related to AI technology are not expressly regulated in the ITE Law.

The latest effort that the Indonesian government has made as a countermeasure against AI is the issuance of AI guidelines by the Minister of Communication and Information Technology. Minister of Communication and Information Budi Arie Setiadi has issued a circular letter on the ethical use of artificial intelligence (AI). Three policies, namely ethical values, application of ethical values, and responsibility in the use and development of artificial intelligence, are contained in the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Ethics of Artificial Intelligence signed on 19 December 2023. Again, it has not been explained the follow-up of the implementation of AI publishing that must comply with the principles of credibility and accountability as mentioned in the content of the circular letter by the Minister of Communication and Information Technology.

In connection with this, so far, although in principle AI is said to be tested for security, there is no further regulation regarding preventive efforts that Indonesia can take to execute it.

3.2. Urgency of Verification Rule as Part of Preventive Law

As we can see, the existing regulation is only repressive and 'punitive' in nature, whereas preventive measures should also be taken to minimise the negative impact of AI. Indonesia needs a legal regulation that more specifically regulates AI and not only mitigates, but also prevents the impact of AI. Law plays an important role as a transformation infrastructure where the law must stand in front as a preventive effort but must also be able to play a role when violations have already occurred (Ramli, 2024b). This makes law as a preventive measure as important as repressive law.

According to Soerjono Soekanto, one of the purposes of law as a social control mechanism is because law is a planned function and uses elements of coercion so that people obey the applicable law (Hukumonline, 2024a). In line with this opinion, expert Philipus M. Hadjon also distinguishes legal protection based on its method, including repressive protection and preventive protection (Hukumonline, 2024b). Protection provided by the government with the aim of stopping offences before they occur is known as preventive protection. It is expressed in laws and regulations intended to prevent offences and provide restrictions or guidance when fulfilling duties (Muchsin, 2003).

Etymologically, prevention comes from the Latin word *pravenire*, which means avoidance or anticipation of something happening. It can be concluded that preventive efforts are social control efforts through the avoidance of disturbances that aim to protect, maintain and control the situation of security and public order. Furthermore, preventive activities or efforts are carried out to ensure that violations of applicable norms do not occur. Referring to this definition, anything done in an attempt to stop something from happening is considered a preventive measure. To conclude, preventive measures are actions taken to stop a violation of the law in a legal context.

Meanwhile, repressive efforts are efforts to recover from disturbances. Any action taken to bring the perpetrator of a crime to justice is an action. Repressive efforts include a series of efforts or actions ranging from investigation, prosecution, examination, to the submission of case files to the public prosecutor to be submitted to the court. Furthermore, the difference between preventive and repressive efforts is that in preventive efforts the instruments used are rules, while in repressive efforts the instruments used are sanctions or punishments. Thus, legal protection is not only repressive but can also be in the form of preventive efforts as a form of prevention before an offence occurs. The inaccuracy of information provided by AI can be said to be unreliable referring to Indonesian positive law (Adinda Putri Denisa, Muhamad Amirulloh, 2023). The obligation of AI service providers to ensure system reliability as Electronic System Operators must be able to guarantee the reliability and security of its operations and the sustainability of the software services it uses (Article 8, PP PSTE). Another obligation stipulates that users and the general public must be protected from losses due to the impact of the electronic system organised by the organiser (Article 31, PP PSTE).

If there is misinformation, the legal position is only between PSE (owner) and PSE (service user), so it is the PSE's obligation to ensure system reliability in accordance with Article 3 paragraph (1) of PP PSTE. Currently, regarding prevention efforts, we can refer to Government Regulation No. 82/2018 on the Implementation of Electronic Systems and Transactions. In relation to software and electronic system requirements in accordance with the mandate of the Ministerial Regulation of the Ministry of Communication and Information Technology of the Republic of Indonesia in 2015, Software Requirements include 13 (thirteen) requirement areas including: Authentication; Session Management; Access Control; Input Validation; Cryptography in Static Verification; Error Handling and Logging; Data Protection; Communication Security; HTTP Security; Malicious Code Control; Business Logic; Files and Resources; and Mobile Applications.

These efforts have sufficiently validated the data in administrative and technical terms, but have not been able to reach AI because there are still procedures related to the application that lean towards business under the auditor set by the minister, thus not reaching AI automated systems that can work on their own even if they are issued under a certain domain/institution(Hetty Hassanah, 2021a).

The Mark Walters vs. *ChatGPT* case is one example of a case that led to a defamation lawsuit over inaccurate AI information. It started when Fred Riehl, a journalist, summarised a federal court case with the help of ChatGPT, which gave errors in the details of the case, resulting in inaccurate information that Walters was involved in the case. Walters was said by ChatGPT to have embezzled over $5,000,000 from a non-profit gun rights organisation called the "*Second*

Amendment Foundation". In fact, Walters was never mentioned or accused in the case at all. This was discovered after Riehl confirmed the validity of the information, thus revealing the true facts before publishing the information.

Learning of the defamatory information, Walters subsequently filed a lawsuit against *ChatGPT* (Vincent, 2023). The CEO of *OpenAI ChatGPT*'s only response to the disinformation was a warning that the system "may occasionally produce incorrect information" and that this had been informed on the *ChatGPT* homepage and said that *ChatGPT* was a reliable data source organised by the company. The case illustrates the invalidity of information and the possible losses that AI service users can incur due to smart machines that process themselves outside of the control of the organisers (Gio Arjuna Putra, Vicko Taniady, 2023).

3.3. Potential Application of the Verification Rule by the United States as a Legal Comparison with Indonesia

Meanwhile, the United States (US) on 30 October 2023, has issued an *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence,* which contains a number of standards in the use and development of AI. This product is a legal product in the form of a Presidential Regulation to regulate AI. The Joe Biden administration's new rules are said to be the strongest imposed by the country regarding the application of AI, said White House Deputy Chief of Staff Bruce Reed. The new draft regulation has been in the works for the past few months, under *Blueprints For an AI Bill of Rights* (CNBC, 2024).

Referring to *Blueprints For an AI Bill of Rights*, AI guidelines are published with the aim of proactively and continuously protecting society from harm, such that "*Automated Systems must be safe and effective by avoiding the use of data that is inappropriate or irrelevant to the task at hand, including reuse that may cause more harm, and by demonstrating the safety and effectiveness of the system* (Blueprints For an AI Bill Of Rights, n.d.)*."*

Mentioned in the *Blueprints for an AI Bill of Rights*, content verification procedures are important in dealing with AI. Unlike Indonesia, which classifies AI as "Electronic Agents", referring to the *Blueprints For an AI Bill of Rights,* AI is classified as an "*Automated System*" or in Indonesian, an automated system with a definition:

*"Any software, process, or system that uses computing entirely or in part to decide, make or support choices, guide the application of policies, gather data or observations, or communicate with people and/or communities is referred to as an "*automated *system." Automated systems exclude passive computer infrastructure and include, but are not limited to, systems built using machine learning, statistics, or other data processing or artificial intelligence approaches. Any intermediary technology that does not affect or determine decision outcomes, make or assist decisions, inform the implementation of policies, or gather data or observations is referred to as "passive computing infrastructure." Examples of this type of technology include web hosting, domain registration*(Hetty Hassanah, 2021b)*, networking, caching, data storage, and cybersecurity. Only those automated systems that are deemed to be within the scope of this framework have the capacity to materially affect people's or communities' access, rights, or opportunities."*

Based on this definition, it can be seen that AI, which is defined as an automated system, covers various forms, including software, as well as processes that use computation, and is not limited to machine learning systems. The definition outlined against the interpretation of AI is more comprehensive and reaches more complex aspects as the development of the form of AI itself. Furthermore, still in the same reference, there is also a definition of algorithm discrimination as part of the impact of AI that can reach *deepfakes*, which can harm people depending on certain circumstances, "*based on race, colour, religion, age, gender identity, disability, ethnicity, national origin, genetic information or other matters expressly protected by law*".

Furthermore, it is mentioned that preventive efforts that can be made by the US community can refer to the *Standard Operating* Procedure (SOP) in the form of:

1. *Consultation.* Consultation with experts when issuing business/application in certain *automated system decision* sectors;
2. *Testing.* Extensive system testing before deployment;
3. *Risk Identification and Mitigations.* Identification of potential risks and risk mitigations (impacts on community rights, opportunities, access, and includes indirect risks to communities outside the sector);
4. *Ongoing Monitoring.* Continuous monitoring during the lifetime of the automated system in use;
5. *Clear Organisational Oversight.* There should be an entity responsible for the development or use of automated systems based on clear governance structures and procedures;
6. *Relevant and High-Quality Data.* Data used for input must be relevant, review of data sources obtained and carefully tracked, restriction of sensitive domain data to minimise dissemination steps and increase adverse impact;
7. *Independent Evaluation.* Enables independent evaluation of automated systems (interface of application programmers, researchers, journalists, ethics review boards, inspectors general, third-party auditorials);
8. *Reporting.* Reporting that is done periodically by the automated system provider.

This SOP can apply to AI as a whole to ensure that AI products that are to be released can ensure the safety and effectiveness of AI and minimise the negative impact of possible unforeseen effects of AI development. This measure can be implemented in Indonesia as a recommendation that there are preventive measures that can be taken in relation to the prevention of disinformation. Of course, the enactment of this measure is also expected to further select AI publishing as a whole which is more effective.

In Indonesia, to be able to implement SOP governance, the most ideal legal product is a Ministerial Regulation. The reason for this is because Ministerial Regulations (Permen) have more flexible rules, can apply in more detail, are easier to revise, and the authorised ministry can regulate more specifically.

Referring to the amendment of Law Number 15 of 2019 on the Amendment to Law Number 12 of 2011 on the Formation of Laws and Regulations, ministerial regulations are explained as regulations stipulated by the minister for the purpose of organising certain affairs of government based on the content material (Explanation of Article 8 paragraph (1)).

In theory, delegation of authority is used to create Ministerial Regulations, which are statutory regulations. This means that the formation of these two laws depends on the delegation of authority to do so from higher laws and regulations. If they have orders from the law, government regulations, or presidential regulations, then ministerial regulations can be formed. This aims to elaborate in more detail and clarity the implementing regulations that are subordinate to the parent regulation.

In addition, the implementation of AI verification rules governance can be realised in several options in relation to delegation/authorisation from higher regulations. The first option can be pursued through the National Strategy, it has been mentioned earlier that the National Strategy for Artificial Intelligence 2020-2045 is currently in the process of becoming a draft Presidential Regulation. If the Strategy can be realised into a Presidential Regulation, the delegation of authority can be done from the Presidential Regulation to the Ministerial Regulation.

The second option can be pursued through the ITE Law. As mentioned earlier, the ITE Law has defined AI as an "Electronic Agent" although it has not specifically regulated the responsibility of this. If the ITE Law is revised, the delegation of authority can be done from the ITE Law as Lex Generalis to the more specific Ministerial Regulation.

The third option is to rushed the *Artificial Intelligence* Law (AI Law) which is expected to address AI issues more comprehensively before delegating more detailed governance to Ministerial Regulations.

The fourth option is to revise some of the Articles and provisions of the software requirements that have been listed in PP PSTE to be able to better reach AI as an automated system and can fulfil the public's right to obtain valid information through AI services with the obligation of PSE to guarantee the reliability (feasibility) of the electronic system offered must be seen as a whole regulatory framework.

By optimising governance further than preventive efforts, it is expected that AI can continue to develop in line with development but can also be controlled so as not to cause more significant harm. In addition to the presence of preventive regulations, special institutions or units with a preventive-anticipatory approach are also important to minimise the impact on the one hand while optimising the benefits of AI on the other. To avoid increasing the burden on the state related to the establishment of new institutions, AI units can be integrated into or add functions to institutions that have been the national digital regulators.

4. CONCLUSION

Based on the author's analysis, it can be concluded that currently the regulation of AI in Indonesia is still limited to the ITE Law as *Lex Generalis* without any further regulation. When referring to the United States AI guidelines, SOPs have been further regulated as a preventive effort in order to reduce the rate of negative impacts of AI in order to ensure the validity of information. These efforts are expected to be recommendations for preventive control for Indonesia, to realise these efforts can be realised in several options. The first option can be pursued through the National Strategy, it has been mentioned earlier that the National Strategy for Artificial Intelligence 2020-2045 is currently in the process of becoming a draft Presidential Regulation. If the Strategy can be realised as a Presidential Regulation, the delegation of authority can be done from the Presidential Regulation to the Ministerial Regulation. The second option can be pursued through the ITE Law. As mentioned earlier, the ITE Law has defined AI as an "Electronic Agent" although it has not specifically regulated the responsibility of this. If the ITE Law is revised, the delegation of authority can be done from the ITE Law as Lex Generalis to the more specific Ministerial Regulation. The third option is to rushed the *Artificial Intelligence* Law (AI Law) which is expected to address AI issues more comprehensively before delegating more detailed governance to Ministerial Regulations. The fourth option is to revise some of the Articles and provisions of the software requirements that have been listed in PP PSTE to be able to better reach AI as an automated system and can fulfil the public's right to obtain valid information through AI services with the obligation of PSE to guarantee the reliability (feasibility) of the electronic system offered must be seen as a whole regulatory framework.

REFERENCES

Adinda Putri Denisa, Muhamad Amirulloh, and N. M. (2023). Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik. Jurnal Rechtsvinding, 12(2), 167–184.

Ahmad Ramli and Tasya Safiranita. (2022). Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi Dan Kebijakan Digital. Refika Aditama.

Blueprints For an AI Bill Of Rights.

CNBC. (2024). Joe Biden Bikin Aturan Ai, Kominfo Blak-Blakan Kondisi RI. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20231031153614-37-485230/joe-biden-bikin-aturan-ai-kominfo-blak-blakan-kondisi-ri

Ellen Kusuma and Nenden Sekar Arum. (2022). Meningkatnya Kekerasan Berbasis Gender Online Setelah Satu Tahun Pandemi Di Indonesia. Yayasan Kesehatan Perempuan. https://ykp.or.id/meningkatnya-kekerasan-basis-gender-online-setelah-satu-tahun-pandemi-di-indonesia/

Feliany Kowanda, Miranda Risang Ayu Palar, L. R. (2024). Pelindungan Hukum Atas Monetisasi Koreografi pada Program Tantangan Menari yang Diunggah Dalam Platform Tiktok. Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik, 2(3), 80–94. https://doi.org/https://doi.org/10.51903/jaksa.v2i3.1880

Floridi, E. H. and L. (2023). The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction - Minds and Machines. Springer Link. https://link.springer.com/article/10.1007/s11023-023-09625-1

Galih, Y. S. (2019). Yurisdiksi Hukum Pidana Dalam Dunia Maya. Jurnal Ilmiah Galuh Justisi, 7(1), 59. https://doi.org/https://doi.org/10.25157/jigj.v7i1.2138

Gio Arjuna Putra, Vicko Taniady, I. M. H. (2023). Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya. Rechtsvinding, 12(2), 281–299. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v12i2.1258

Hetty Hassanah, W. W. (2021a). Pengakuan Putusan Penyedia Layanan Penyelesaian Sengketa Nama Domain Asing. Jurnal Bina Mulia Hukum, 6(1), 34–46. https://doi.org/10.23920/jbmh.v6i1.240

Hetty Hassanah, W. W. (2021b). Prinsip-Prinsip yang Harus Dipertimbangkan dalam Penyelesaian Sengketa Nama Domain Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan, 12(1), 43–58. https://doi.org/10.22212/jnh.v12i1.1743

Hukumonline. (2024a). Perbedaan Upaya Preventif Dan Represif Serta Contohnya. Hukumonline.Com. https://www.hukumonline.com/berita/a/upaya-preventif-lt63e0813b74769/.

Hukumonline. (2024b). Teori-Teori Perlindungan Hukum Menurut Para Ahli. Hukumonline.Com.

Imamulhadi. (2017). Ikhtisar Ilmu Hukum. K. Media.

Kristophorus Hadiono, R. C. N. S. (2020). (Kristophorus Hadiono dan Rina Candra Noor Santi, 2020). Unisbank.

Maudy Andreana Lestari, Ahmad M Ramli, and T. S. R. (2022). Telaah Yuridis Penyelenggaraan Teknologi 5G Di Indonesia: Langkah Transformasi Menuju Era Society 5.0. Citizen : Jurnal Ilmiah Multidisiplin Indonesia, 2(1), 129–137. https://doi.org/https://doi.org/10.53866/jimi.v2i1.49

Mediana. (2023). 'deepfake' Yang Mencemaskan,. Kompas.Id. https://www.kompas.id/baca/ekonomi/2023/11/05/deepfake-yang-mencemaskan

Mochtar Kusumaatmadja, Otje Salman, E. D. (2002). Konsep-Konsep Hukum Dalam Pembangunan. Alumni.

Muchsin. (2003). Perlindungan Dan Kepastian Hukum Bagi Investor Di Indonesia.

Patria, N. (2024). Siaran Pers No. 470/HM/KOMINFO/11/2023 Tentang Antisipasi Deep Fake, Wamen Nezar Patria: Kominfo Lindungi Kelompok Rentan. https://www.kominfo.go.id/content/detail/52967/siaran-pers-no-470hmkominfo112023-tentang-antisipasi-deep-fake

PLEADS FH Unpad. (2024). Perlindungan Hukum Bagi Korban DEEPFAKE Pornografi: Evaluasi Efektivitas Hukum Positif. FH Unpad. https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35

Priancha, Z. P. M. (2024). Pengaturan Hukum Artifical Intelligence Indonesia Saat Ini. Hukumonline.Com. https://www.hukumonline.com/berita/a/pengaturan-hukum-artifical-intelligence-indonesia-saat-ini-lt608b740fb22b7/?page=2

Priowirjanto, M. F. and E. S. (2022). Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia. Jurnal Indonesia Sosial Teknologi, 3(11), 1161. https://doi.org/https://doi.org/10.36418/jist.v3i11.528

Ramli, A. (2024a). Kedaulatan Digital, 'Sovereign Ai', Dan Yurisdiksi Negara (Bagian II-Habis). Kompas.Com. https://tekno.kompas.com/read/2024/05/16/11141467/kedaulatan-digital-sovereign-ai-dan-yurisdiksi-negara-bagian

-ii-habis?page=all#page2

Ramli, A. (2024b). Lembaga Pengawas Dan Pemberi Sanksi Pelanggaran Ai. Kompas.Com. https://tekno.kompas.com/read/2024/04/23/08534247/lembaga-pengawas-dan-pemberi-sanksi-pelanggaran-ai?page=all#page2

Ramli, A. (2024c). Penggunaan Ai Dan Masa Depan Industri Telekomunikasi. Kompas.Com. https://tekno.kompas.com/read/2024/04/28/15363017/penggunaan-ai-dan-masa-depan-industri-telekomunikasi?page=all#page2

Rizki Fauzi, Tasya Safiranita Ramli, R. R. P. (2022). Masa DEPAN Hak Cipta: Tinjauan Keabsahan Hasil Karya Kecerdasan Artifisial Di Indonesia. Citizen : Jurnal Ilmiah Multidisiplin Indonesia, 2(1), 118–128. https://doi.org/https://doi.org/10.53866/jimi.v2i1.51

Santoso, M. R. A. and B. (2018). Urgensi Rekonstruksi Hukum E-Commerce Di Indonesia. LAW REFORM, 14(1), 89. https://doi.org/https://doi.org/10.14710/lr.v14i1.20239

Sari, R. P. (2024a). Apa Itu Deepfake? Kenali Bahaya Dan Cara Mendeteksinya. Cloud Computing Indonesia. https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-deepfake-bahaya

Sari, R. P. (2024b). Kemenkominfo Peringatkan Ancaman Deepfake Ai. Cloud Computing Indonesia. https://www.cloudcomputing.id/berita/kominfo-peringatkan-deepfake

Vincent, J. (2023). OpenAI Sued for Defamation after CHATGPT Fabricates Legal Accusations against Radio Host. The Verge. https://www.theverge.com/2023/6/9/23755057/openai-chatgpt-false-information-defamation-lawsuit

Welle, D. (2024). Deepfake Kelabui Jutaan Calon Pemilih Di Asia Jelang PEMILU. Dunia Digital Asia Dw.Com. https://www.dw.com/id/deepfake-jelang-pemilu/a-67880534

WIPO. (2016). Understanding Copyright and Related Rights, World Intellectual Property Organization, Switzerland.