Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia

Ari Purwadi[1*], Cita Yustisia Serfiyani[2],
Universitas Wijaya Kusuma Surabaya

Citi Rahmati Serfiyani[3]
Airlangga University

Abstract
The utilization of technology is vulnerable to misapplication of digital personal data either from public figures and citizens, one of them is in the form of deep fake technology. The manipulation of video technology in the form of deep fake globally has disrupted large scale disruptions in online networks in some countries such as the United States. The methods already spread to developing countries, which is Indonesia. The misapplication or manipulation of deep fake is not only intended for entertainment or to defame someone's reputation but on a large scale it is also used to form public opinion, divert issues and spread hoax news and cybercrime to incite cyberterrorism. Its existence in cyberterrorism is increasingly growing. This legal research discusses the manipulation of personal data into deep fake technology and its impact on cyberterrorism, political and legal resilience in Indonesia. The comparisons will also be applied to the United States. This research focuses more on preventive methods in dealing with deep fakes in Indonesia in cyberterrorism, namely aspects of counterterrorism, socialization and government literacy, development of preventive technology and strengthening of counter terrorism regulations that must be adjusted to several deep fake characteristics.

Keywords: deep fake, cybercrime, cyberterrorism, cybersecurity, technology and informatics law, Indonesia

Introduction

Technological developments lead to a quality of life that appears in line with its negative impact in the forms of digital-based crimes. Furthermore, the easier it is for

[1] Faculty of Law, Universitas Wijaya Kusuma Surabaya
[2] Faculty of Law, Universitas Wijaya Kusuma Surabaya
[3] Law Faculty, Airlangga University
*Corresponding author

something to be created, the easier it will be for something to be faked. When we flashback to decades ago when paper money, demand deposits and physical securities were the primary commodities in Indonesia in business transactions, responsible parties had emerged to counterfeit these assets. As technology developed and people turned to digital money and digital securities, asset counterfeiting efforts continued to occur but were no longer targeting money and securities but forgery of identity in user accounts where the assets were stored (Muzykant et al., 2021; Wolman, 2013).

The use of information technology in country's digital government service, for instance, makes a good impact on the smooth driving of government affairs on the efficiency and cheaper dissemination of information. However, the opportunity to use information technology for destructive purposes relates to society and legal policies when it is used by cybercriminals for activities like cyberbullying and cyberterrorism, which should be taken into account. Previous research highlighting the relationship between deep fake technologies in cyberterrorism activities is increasingly worrying (Antinori, 2019; De Ruiter, 2021; Yu & Carroll, 2021). By using deep fake technologies, all acts of cyberterrorism that occur will be more destructive in its existence, not only change form but also have the capability to constantly adapt to the dominant tools used by cybercriminals. The cyberterrorists can exploit political, cultural and social problems on the internet and information technology as the mass propagation of hoaxes and disinformation aimed at reducing the credibility and integrity of certain individuals or institutions (Howard, Woolley, & Calo, 2018; Nastiti et al., 2018) Cyberterrorists can spread hoax news with various methods ranging from fake news narratives on blogs, the web, social media, falsifying news sources, documents, and photo documentation to achieve their political or ideological gains. This is related to a main feature of deep fake technologies, extended to the falsification of someone's identity recorded on video by deep fake engineering, an issue which is the focus of the current discussion.

Deep fakes in cyberterrorism are carried out in a series of black large-scale disruption of computer networks (Hower & Uradnik, 2011). In addition, the convenience of the internet makes it easier to make mass duplication of anonymous accounts to broadcast videos, clickbait, subliminal messages, and negative affirmations to the public (Akhgar, Staniforth, & Bosco, 2014; Hasen, 2019; Schick, 2020). Concerning online large-scale disruption of computer networks, this risk factor is also compounded by the difficulty in tracking the users and real activities used during online activities. Deep fake technology also makes it easier for cyberterrorists to access the financing and funding resources, by bridging illegal transfers and illicit trading through non-conventional online platforms (Levine, 2020; Teichmann, 2018). This challenge will be more difficult for counter terrorism agencies in developing countries such as Indonesia as the limited skill and capability in acquiring the latest development of deep fake technology in counter terrorism strategies. For instance, in term of illicit trading and money laundering, there are difficulty in tracking the real activities used during online activities. This is because transactions on the internet do not only recognize rupiah currency, demand deposits, and digital money that the Central Bank of Indonesia (hereby abbreviated as BI) can track, but it can also be done with cryptocurrencies outside the authority of BI because the cryptocurrency is not a legal currency that applies in a country including Indonesia.

Another feature provided by deep fake is through face recognition technology. Nowadays, e-government services and services provided by private parties currently utilize the sophistication of face and voice recognition through the aid of artificial intelligence so that the characteristics of determining human faces and voices as their unique identifiers will be stored in the service provider's system database (Westerlund, 2019). The recognition points of human faces can be obtained through face recognition technology taken on purpose and captured through photos uploaded by the subject in question. The face can then be misused onto other media using the app. This technology is then called deep fake technology (Lai & Rau, 2021).

Rationale/ Research Objectives

The use of deep fake technology is now not only about pornography, political activities and hacking, especially if the facial identity used is the face of well-known political and government figures or institutions in the eyes of the public but also in the area of cyber terrorism. Deep fakes misuse personal identities through video manipulation without permission. For instance, the 2016 United States election case, deep fakes have also been used to represent famous politicians on video portals or chatrooms. For example, the face of Argentine President Mauricio Macri can be replaced by the face of Adolf Hitler, and Angela Merkel's face is replaced with that of Donald Trump to create fake news in the political and legal fields (De Maio, 2019).

Deep fake technology can also be used by cybercriminals as it provides many features to easily conduct violent acts in order to achieve political or ideological gains by threatening the social or political institutions or significant bodily harm for propaganda purposes. By using deep fake technologies, cybercriminals can hijack vital sites to carry out the action. In addition, piracy of social services, theft of cryptocurrencies and disruption of the banking system can be carried out by cyberterrorists to disrupt economic, political and social stability (Dion-Schwarz, Manheim, & Johnston, 2019; Teichmann, 2018; Westerlund, 2019). Also, it aims as propaganda to undermine the capabilities of the internet system, national security and the reputation of legitimate institutions (Kfir, 2020).

The utilization of information technology in cyber terrorism in cyberspace is a worrying phenomenon that needs a serious attention from stakeholders. Especially after the countries in the world have experienced the COVID-19 pandemic since 2020, people and countries are forced to use information technology in their daily activities. This leaves society in general vulnerable to cyberattacks by leveraging technology deep fakes. The frequency of use of digital platforms and the use of personal computers attached to the internet by users can be exploited by cybercriminals to steal data and spread computer worms, phishing, malware, malicious software, and computer viruses. Various programming scripts and hardware methods can be used as tools for internet terrorists (Talihärm, 2010; Wilson, 2008).

With deepfake technology, the virtual world will gradually develop into a new world reality for humans that has the same influence as the real world (Veerasamy, 2020). It becomes a new challenge for the government so that the legal protection provided in cyberspace must be as strict as the legal protection applied in the real world. Counter terrorism strategies need to be adapted with this new development. Therefore, this study will discuss the legal protection aspects of the misuse of personal data into deep fake technology, which can impact national security in the cyberterrorism.

Literature Review

- *Deep Fake Technology in the Misuse of Personal Identity*

The news circulated on the internet cannot be fully legitimized even though it is spread byaccounts that have broad influence. Hence, the crux of the problem the quality of information andnews on the internet is about which information is right and wrong and who has the right to legitimize which information is correct (Allcott & Gentzkow, 2017). Fake news can be broadly classified into three categories, misinformation (accidentally and misunderstood in responding to and spreading news), mal-information (deliberately using genuine and good news for bad purposes), and disinformation (intentionally taking advantage of the news to change the perception of the actual reality) (Lestari & Sari, 2020). Deep fake in video engineering aims to create disinformation (Whyte, 2020).

The term “deep fake” originates from a combination of the words "deep learning" and "fake." The meaning of deep learning is deep and structured learning with machine learning methods based on data representation but contrary to specific algorithms. Deep learning uses a layered algorithmic structure called an Artificial Neural Network (ANN). The main character of deep fake is that the software used must be based on artificial intelligence (AI) to swap one subject's face as a source to another subject in the form of video as an external target. AI, through computer programs, can also be realized in hardware to complete tasks related to human-like perception, cognition, and communication because AI can think like a substitute for the human brain and body through a series of binary codes in programming logic.

When the first discovery, AI was considered a technology that was able to think like humans; now, the perception of AI has developed into a technology that is able to act like humans (Sayler, 2020). AI is not fundamentally the same as robots, but AI can be used to build robots. AI has several unique characteristics; namely, it has the potential to be integrated with various applications, improvising technological advances based on the internet of things (Brantly, 2018), and able to be applied in the affairs of public services to the military resilience of a country. For example, the United States uses facial recognition algorithms to recognize the faces of people as suspected terrorists during the conflicts in Syria and Afghanistan (Allen & Chan, 2017), and can also be used for the administration of the occupation in making identity cards of residents in Indonesia.

The following characteristic of AI is distortionary engineering of data into machine learning. Although both can be used for engineering, deep fakes and CGI are technically different.The use of AI into deep fake technology allows creators to easily apply a person's face to another person's body in a series of images that become a video. The more data sets we have, the easier it will be for the forger to create deep fake videos that are more similar and more convincing to the public. CGI is more like traditional animation techniques. In traditional animation techniques, a movement is created through a series of interlocking images generally in a rhythm of 24 fps (frames per second), meaning that 24 images are assembled to create animation within 1 second. CGI has made it easier for manual animation work to merge images into videos that were previously done manually can now be done computerized. On the other hand, deep fake is a video engineering technique that utilizes artificial intelligence, primarily machine learning, where there is a special algorithm used to

train machine learning to understand a person's facial movementson video and compare them with the photos provided as a database. The database has the function to move one object to another in order to resemble it closely.

Engineering through deep fake is executed by collecting as many photos as possible of the figure whose face is about to be replaced with a photo of the figure whose body will be plastered with the new face. Next, the photos are then the creators distort the photos in the database to enable machine learning analysis capabilities to find characteristics and look for similarities. The intentionally distorted database analysis process causes machine learning to experience blurry information to assume the figures are the same. Machines that can carry out machine learning processes can be purchased for a fee or for free on open source-based sites so that gradually deep fake techniques are easier to comprehend by the younger generation who are more technology literate. Some applications that can produce deep fake videos easily are Zao, Avenge Them, Deep fakes Web, Doublicat, Machine Tube, Face2Face, although their priority is forentertainment purposes. Unfortunately, videos engineered by deep fakes are not entirely of high quality and far below the quality of videos produced by CGI technology, which; the ease of making deep fakes makes deep fakes more dangerous because they are easier to reach and apply to all walks of life.

- *Legal Protection of Misused Personal Data Through Deep Fake Technology*

Deep fake technology was first widely known from the political world (Yerlikaya & Aslan, 2020). However, its familiarity with the digital-based crimes are also rapidly growing in many social aspects such as cyberterrorism (Antinori, 2019; Dawson, 2015). For instance, although the United States has implemented the online election voting mechanism, it is still distorted by the spread of hoax news and deep fake videos because some 14% of Americans still consider the internet to be an essential news source, and the public is proven to be more likely to believe stories that support their chosen candidate regardless of the truth the news (Allcott & Gentzkow, 2017). Moreover, even 39% of the world's globally do not review the information and videos they receive (Barometer, 2021).

The Indonesian people are also vulnerable to hoax news, including deep fake videos. Based on the Edelman Trust Barometer survey, countries that are dreaded to be targeted for usinginappropriate/ wrong digital information are Indonesia, Mexico, Argentina, and Spain, with the percentage of concern ranging from 76 – 80%. Based on a survey conducted by the Indonesian Telecommunications Society, 44% of people receive hoax news every day, and 91.8% of the types of news received are socio-political aspects related to the central government and local governments (Indonesia, 2019). Since the beginning of independence in 1945, Indonesia's political views have been influenced by changes in the legal policies of legislators. Then over time, the dissemination of information online also enlivened activities in the social arena. In the past, campaign activities were carried out directly, all face-to-face actions in power-raising were determined by how influential a person was in the real world, but now online cyberterrorism are generally carried out through online campaign activities, polls, and online vote surveys, online election voting.

On one hand, Indonesia has not dared to take progressive steps in fully implementing online elections. However, the involvement of information technology

in campaign activities in Indonesia has been very evident in the country's political activities. The dissemination ofpolitical propaganda, and online campaign activities, particularly during the COVID-19 pandemic throughout 2020, which forced the public to carry out the majority of its activities via online (Rahmanti et al., 2021). The digital age has changed the way countries conduct political warfare and necessitate a rebalancing of security priorities in democracies (Paterson & Hanley, 2020). The effort to reach every Indonesian citizen through gadgets is much easier than gathering the masses directly. The dissemination of information online is the option that many practitioners of the political world choose today, regardless of the condition before, during, and after the Covid-19 pandemic.

Deep fakes can be used to bring down a person's personal image to meddle the economic and political conditions of a country depending on the purpose of its use. There are at least four main types of deep fake producers: (1) Deep fake hobbyist communities; (2) Political players such as foreign governments and various activists; (3) Other bad actors such as fraudsters; and (4) Legitimate actors such as television companies for entertainment purposes only. The negative impact of deep fakes can also be provoked by the tendency of people's attitudes inresponding to hoax news on the internet. They often do not considerately track the source, nor the truth, and purpose of the news so that a video engineered by deep fakes, no matter how high or low the quality is, still can begin misinformation and mal-information, and disinformation in society. The majority of Indonesian people, around 63.3%, still believe that news and videos must be trustworthy if they are spread by trusted sites and people (Indonesia, 2019).

The following deep fake character is that the primary purpose of making videos is to influence people's mindsets through the concept of "seeing is believing." Therefore, the main purpose of making videos through deep fake is not to pursue the perfection of video quality but to quickly and easily influence the mindset of people in the majority by utilizing the concept of "seeing is believing." As a result, even though the quality of the video produced is not perfect, thehuman brain can still be convinced even with a lie and fake event. The naked eye can still distinguish deep fakes between fake and real ones, yet if deep fake technology is perfect, it will be complicated to manage or distinguish between real and fake ones.Hence, Google and Facebook have made attempts to prevent the development of deep fake by sharing a database of 3000 deep fake videos analysis results that can be used by researchers and experts in the field of information technology to find loopholes in stopping the production and distribution of deep fake videos.

Addressing face recognition and video recognition used as the basic idea of deep fake technology, facial recognition processing is now considered standard for entertainment purposes. For instance, face swab applications, Snapchat to Instagram filters without realizing the dangers of misuse of face recognition and voice recognition. One of the countries that often use facial recognition technology, face scans, or face swaps is the United States. The United States and China are pioneers of the intensive use of facial recognition in the interests of state administration, but this seems to have sparked a debate in recent years due to the commercial use of face and voice recognition technology. Based on data from the Mordor Intelligence survey in the United States, the facial recognition and face scan industry, especially for citizen

surveillance and business product marketing, grew $4.8 billion in 2020 and is expected to increase to $12.75 billion in 2026 in the United States (Intelligence, 2021).

The application of deep fake can be managed for positive or negative purposes. However,deep fake technology that are applied for negative political purposes will be more likely to violate the rule of law and norms. As an illustration, the video engineering deep fake in the election between Trump and Clinton in 2016. Harmful conduct of deep fake also occurs in cybercrime, which extends to e-terrorism and cyber-social terrorism that use technology manipulation as a digital weapon for propaganda purposes (Antinori, 2019). The act of e-terrorism is deemed more effective because of the current pattern of people's lives that rely profoundly on technology and voluntarily submit their personal data to site and application providers in one big data unit.

Aside from the negative impacts and controversies that have occurred, deep fake technology is also able to provide benefits and have prospects in other fields, especially in the fields of entertainment and business. For example, Deep fake technology can advance the entertainment industry from filmmaking, educational media, digital communication, games, development of social media applications, providing improvements for health services, online business promotion, and graphic design developments to develop e-commerce sites.

The deep fake technology enables dubbing a person's original voice in film productions, especially when reproducing older films. Deep fake technology can also be a voice over solution in teleconference meetings conducted by various foreign languages, increasing the ease of communication in social media to the chat forum feature in multiplayer-based games. Deep fake in the health sector can help people with Alzheimer's interact with people's faces and their faces that have been forgotten in their long-term memory. Deep fakes can also help the business world in the development of e-commerce features and online marketing. There are more immense possibilities for developing deep fake technology in the future as long as the positive andnegative aspects of using this technology can be separated wisely, professionally, and obey the law.

Therefore, the legal protection of people's personal data that is misused through deep fake technology and its impact on the political and legal resilience of a country is an urgent matter to be studied and relates to the characteristics of deep fakes, namely: (1) AI involvement, (2) distorted data engineering through machine learning, (3) the purpose of communication is to manipulate a person's mindset through the concept of "seeing and believing," and (4) use for activities that violate legal norms and the rule of law.

Research Method

This study seeks to analyze the handling of cybercrime in the misuse of personal data through deep fake technology, especially in cyberterrorism. The theoretical model is framed from the formulation of legislation in Indonesia in dealing with violations and cyber-crimes through the Information and Electronic Transaction Law no. 11 of 2008. In general, the theoretical framework in this study focuses on a socio-juridical approach, which seeks to conceptualize social phenomena in terms of the legal aspects of technology deep fake crimes. In general, some of the problems that

need to be underlined from technology deep fakes in Indonesia are counterfeiting financial assets, data leakage, personal data protection, spreading hoax news, and falsifying digital data. This then develops into the misuse of technology that is able to shape a new reality that is very different from the facts in the world in a manipulative way. The process of creating a false reality in cyberspace is used in cyberterrorism to direct public opinion. This makes technology deep fake crimes related to the cyberterrorism aspect, where public attention is on the need for data protection and more progressive legal arrangements regarding technology deep fake cyber-crimes.

The analysis used in this study is descriptive analytical with a qualitative approach with several identification steps. The first step is to identify socio-political developments that point to the dangers of deep fakes in Indonesian politics. The second step is to identify laws related to information crimes in Indonesia. Several laws that are used as a reference in this study are the Electronic Information and Transactions Law. The positive law in question is the relevant law currently in force, namely the Criminal Code, Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), and Law Number 5 of 2018 concerning Eradication of Criminal Acts of Terrorism. The analysis is specifically carried out with qualitative methods by collecting data related to cyber-crimes of deep fake technology, reducing the data and presenting them in conclusions.

Results

Deep fake is more than just a common hoax because it can modify content, manipulate images, and distort information. Deep fake attempts to mix half-truth information with half-truth, but what is intended is the lie through engineering facial expressions, gestures, and voices similarto the original. Deep fake can forge CCTV footage, falsify the audio recordings in courtrooms, and counterfeiting video recordings of a religious leader. One example of a deep fake video thatis intentionally spread for political purposes is a video of a speech by former US President Barack Obama in 2018 which insulted US President Donald Trump (Vaccari & Chadwick, 2020), even though the video was made for entertainment purposes, no one can predict the extent of the impact and how massive the sharing between smartphone users on that one video is.

Deep fake is only one of the several sophistications produced by the birth of artificial intelligence technology (artificial intelligence) in digital processing data. The use of AI is steered in business, entertainment, and education and has also been directed to political interests, determining the direction of a country's legal policy, and strengthening its military resilience. Countries that have implemented AI for military defense and resilience are the United States through the U.S. National Defense and Russia, while China has prepared the use of AI into the military field of its country for the year 2030 into the future (Sayler, 2020). AI technology in the United States is primarily to strengthen the country's cyber resilience against cyberattacks from other countries and strengthen the country in physical attacks. The U.S. National Defense, for example, has been able to implement the Maven project to identify fugitive targets in areas far from home during theconflicts in Iraq and Syria (Ramanouski, 2019). The use of AI by the United States has begun to be regulated in general in the FY2019 National Defense Authorization Act (NDAA).

Indonesia is an integral part of the so-called "global swing states" or countries that can determine the direction of world political and economic movements (Kliman, 2012). The alleged involvement of the United States in global swing states, including Indonesia (Fontaine & Kliman, 2013), become more assertive with the support of sophistication in information technology so that the boundary between digital information intended for public consumption and data privacy is becoming vaguer. The use of digital data processed using artificial intelligence is easy to reach because it is supported by big data technology that makes it easier for certain parties to collect individual personal data with the refinement of data processing, storage capacity, and unlimited access both consciously and voluntarily or unconsciously. Big data not only makes life easier with one-touch but also risks misuse of data in one touch as well. Big data collects call data, transactions, career history, medical history, GPS location to political choices, and a person's favorite artist. Big data, in many directions, help in discovering social phenomenon and social facts quicker than manual surveys because big data can simplify the process of predicting metadata (Crawford, Miltner, & Gray, 2014). On the other hand, data stored collectively by a party is also at risk of being lost and misused either by the party in charge or by a third party.

Indonesia is currently still a potential target for cyber-attacks and malware from other countries in the Asia Pacific and domestically because it still occupies the second position as the country with the most potential for ransomware attacks (Microsoft, 2019). It will be significant if the data coverage is enlarged to international. This circumstance can place Indonesia as a country that is still vulnerable to opportunities for online criminal acts of cybercriminals, including cyberterrorism, e-terrorism and cyber-social terrorism. Moreover, the spread of deep fake that is not appropriately anticipated can cause Indonesia to be in a crisis of ideology, politics, economy, social culture, defense, and security (Azali, 2017).

In politics, the use of deep fakes for politicized interests by irresponsible parties affects the credibility and quality of a country's democracy. The circulation of deep fakes comes from domestic political competition and can also come from other countries that deliberately want to interfere with the political and economic conditions of a country. Setting words in someone's mouth on a viral video is a powerful weapon in today's war of disinformation because the altered video can easily distort voter opinion, for example, through a fake video about a politician. In addition, various political players, including political agitators, hackers, terrorists, and foreign nations, can use deep fake in disinformation and large-scale disruption of computer networks to manipulate public opinion and undermine trust in certain state institutions.

For cyberterrorism, the existing effect obtained from deep fakes in political spheres is considered beneficial for advancing their political and ideological propaganda. Nowadays, digital applications have been substantially growing in society. Implementing digitalized society as the latest development of information technologies is not a static concept but an adaptive concept. It still demands the role of the government in cultivating an excellent digital culture to prevent users to access deep fake technology to incite cyberterrorism. The government can create deep fake countermeasures from 3 (three) aspects, namely; (1) providing literacy to the public, (2) developing AI-based technology as well as analyzing and preventing thespread of deep fakes, and (3) establishing new regulations to arrest perpetrators and spreaders of deep fake and consistent ITE law and anti-terrorism law enforcement.

Indonesia can start anticipating socialization, literacy, and intensive education in the community and to raise awareness and digital literacy regarding the harmful effect of deep fakes in cyberterrorism. Indonesian people are still not independent in analyzing the validity of hoax news and deep fake videos because 31.9% of the people still need government assistance for official corrections/clarifications on social media about the fakeness of a video, not based on their knowledge and awareness, then 83% seeking clarification in cyberspace, not in printed news or real-world interactions (Indonesia, 2019). Literacy on the dangers of deep fakes is an effective prevention method considering that technological developments often develop faster than new legal regulations regulating them.

Recent research from the United States (US) shows that people over the age of 65 and with conservative political views have a higher tendency to spread false news or hoaxes through social media (Guess, Nagler, & Tucker, 2019). The United States government's preventive efforts require the role of digital media (Taylor, 2021). Besides taking a role in disseminating educational information about the prevention of deep fakes, the tendency to quickly spread deep fakes also influences the level of public trust in the credibility of digital media, which in their daily lives are tasked with publishing news digitally to the public. Research conducted in the United States that politically charged deep fake videos deceived 50% of the 5,750 respondents due to a lack of political literacy and information technology (Barari, Lucas, & Munger, 2021).

In Indonesia, the correlation resembles the total duration of internet usage per person and their level of belief in conspiracy theories (Indonesia, 2019). This is in line with research that states people who tend to spread hoaxes are people who use the internet more often and have longer durations, and the higher a person's belief in conspiracies also increases the tendency to spread hoaxes (Brotherton, French, & Pickering, 2013). In spreading conspiracy theories, even videos edited without involving deep fake technology can stillharm the community targeted by the video creator. For instance, when the video about theburning *Qur'an* and Islamic religious books by the United States Army in Afghanistan spread, even though the United States stated that the truth on the ground was not as clear as the situations shown in the short video (Chesney & Citron, 2019).

Videos like such are used to become propaganda tools for cyber terrorists who want to significantly change the established political or social orders for their ideological or political goals. A picture may be worth a thousand words, but nothing is as convincing as an audio or video recording of an event. Currently, digital information has played a role like swords and firearms in digital warfare, while protection from the state acts as a shield for people who absorb the information without a filter. Especially if the video distributed is engineered in terms of faces, gestures, and sounds, it changes the video's substance. That is why the public requires to find alternative sources of information and juxtapose them with the news content to confirm the truth of the information (Aufderheide, 2018).

Technical solutions to AI-based technology that Indonesia can do to prevent the spread of deep fake videos, especially in cybercriminals, including cyberterrorism, e-terrorism and cyber-social terrorism by using the steganography method distinguishes between original videos and fake or edited videos. Steganography is the art and science of hiding information by embedding a message within another

seemingly harmless message. Steganography operates by replacing useless or unused data in ordinary computer files (such as graphics, sound, text, HTML, or even floppy disks) with different, invisible bits of information. This hidden information can be plain text, cipher text, or even images. Steganography is vital because inserting data in images, text, or documents is only known by the owner who uses this steganography. Another method is to use a Convolutional Neural Network (CNN)-based application system that trains a Recurrent Neural Network (RNN) system that acts like the human brain in classifying video authenticity and fakeness. Techniques like this cannot be applied by individuals but must be carried out through institutions with adequate capabilities. In America, for example, there is an institution called DARPA, which has launched a project called Media Forensics (MediFor) to detect and provide detailed information about deep fake video manipulation.

The subsequent prevention and countermeasure are from legal protection. Counterterrorism regulations must be strengthened by increasing the capacity and capability of counterterrorism agencies to adopt latest technology of deep fakes. This legal protection must be given to all digital information and digital data, and both shared consciously and according to the agreement of the owner (data consent) and digital data that is shared unknowingly, without permission, or without agreement by the owner (data non-consent). This will be likely to limit the capability of cybercriminals to incite cyberterrorism, e-terrorism and cyber-social terrorism. The regulatory aspects of the internet and artificial intelligence are the most critical coping factors. However, no regulation explicitly regulates the misuse of deep fake technology or artificial intelligence (AI) in Indonesia. The absence of legal measures is also reflected in counterterrorism in combating cyberterrorism, e-terrorism and cyber-social terrorism. However, if there is a distribution or misuse of videos or images engineered by deep fakes, the perpetrators can be charged with the Electronic Information and Transactions Law. The positive law in question is the relevant law currently in force, namely the Criminal Code, Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), Law No. 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination. Regarding which rules should be applied need to be seen again on a case-by-case basis.

Discussion

As to take a progressive measure of deep-fake manipulation from personal identity especially in cyberterrorism, e-terrorism and cyber-social terrorism, legal protection toward misuse of deep fake videos can be done with referring to the protection of the personal data of every citizen. It is the obligation of the government in the current big data era. Thus, the legal rules imposed on creators and spreaders of deep fake video content are no different from the legal rules imposed on creators negatively charged propaganda videos in general. The rules can also be applied to cyberterrorism, e-terrorism and cyber-social terrorism. More specifically, some of the legal bases that can be applied in handling negative content, including deep fake engineering videos, are Article 40 paragraph (2), Article 40 paragraph (2a), and Article 40 paragraph (2b) of the ITE Law, Minister of Communication and Information Technology Regulation No. 19 of 2014 concerning Handling of Negatively Content Sites and if deep fakes contain pornographic content, the provisions of Article 378 of the Criminal Code,

Article 35 of Law Number 44 of 2008 concerning Pornography and Article 45 paragraph (1) of the ITE Law, and Law Number 5 of 2018 concerning Eradication of Criminal Acts of Terrorism can be added.

To combat cyberterrorism, e-terrorism and cyber-social terrorism, the way to determine the law for deep fake cases is through digital forensics. The functionof digital forensics is to expose the strength and validity of evidence in the field of cybercrime, especially Article 5 of the ITE Law, which states that electronic information and electronic documents are legal evidence in Indonesia. The official digital forensic institution in Indonesia is under the Directorate of Information Control, Investigation, and Digital Forensics of the National Cyber and Crypto Agency (BSSN). Digital evidence must pass standardized tests, so the authenticity can be guaranteed and can be accounted for. The primary standard for digitalevidence to be admissible in a judicial process is that it must be accepted and used for legal purposes and interests, original, complete and trustworthy. Digital forensics involves the profession of digital forensic analysts and a set of computer forensics varying from cases of intellectual property rights violations, economic crimes, cybercrimes, including video engineering. In the United States and the Netherlands, for example, video engineering analysis can be done with the degreaser application (Casey, 2009).

The speed of technological improvement in digital forensics is also one of the causes of the difficulty for the government to issue legal regulations that are responsive or progressive to new developments in the field of information technology, especially when the threats from cyberterrorism, e-terrorism and cyber-social terrorism is increasingly developing. As a result, the rule of law is often left behind by the times. The law that develops in society is not a static law but a dynamic law. The legal system is not merely a set of static rules but a constantly changing reflection from developments, especially the relationship of the diversity of social characteristics that live in society, both traditional and modern, both rapid and slow changes. The cyber law to combat cyberterrorism, e-terrorism and cyber-social terrorism must be adapted continuously to prevent the latest development of cyberwar on terrorism. This is in line with the idea that law reflects the diversity of social characteristics. There is no law that does not change and that change always creates conflict. Hence, in this case, the law must be seen as a social engineering tool where the law must adjust to existing changes if it does not want to be left far behind. This continuous effort to develop the legal order is obliged so that there is no legal vacuum for too long and law enforcement is not only passively waiting for written legal rules.

The digital track record is also a law enforcement asset to trace the location of deep fake video makers. As a result, the perpetrators of cyberterrorism in cyberspace will not feel safe to commit criminal acts, especially violations of the ITE Law and Anti-terrorism Law. The collaboration of the Ministry of Communication and Information, the anti-terrorism agencies, and the police headquarters needs to be strengthened to monitor digital track records and the latest strategies and challenges raised by cyberterrorism, e-terrorism and cyber-social terrorism. The logic used in Indonesia in handling the spread of deep fake videos is the same as porn videos which. Although it was used for personal purposes, it can still have a broad negative impact if they are disseminated either accidentally by themselves or by third parties. This impact will

be broader in cyberterrorism as it directly aimed at overthrowing the established political, economic and social orders (Susilo & Dalimunthe, 2019). Therefore, the imposition of punishment is emphasized on its impact, not only on the original intention of making the video. Both the distribution of e-terrorism and other purposes such as pornographic videos made for personal collections and deep fake videos that are politically charged are the same as abusing someone's personal data. In this case, the protection of individual personal data is faced with the intersection between the government's obligation to protect the rights of the individual concerned and the government's obligation to protect the community's interests from cybercriminals, especially cyberterrorism, e-terrorism and cyber-social terrorism.

In the United States and the European continent, personal data protection has been operating well. In Europe, there is a "Right to be Forgotten (RTBF) application mechanism. Articles in the ITE Law related to the right to be forgotten have accommodated arrangements such as Article 17 of the General Data Protection Regulation (GDPR). GDPR is a data protection regulation that is part of European Union law. The right to be forgotten was first regulated in law through the GDPR. The United States has not adopted this in specific legislation and is still based on jurisprudence as a source of law, for example, in the Cox Broadcasting Corp vs. Cohn cases in1975 (Georgia), Garcia vs. Google in 2015, Manchanda vs. Google in 2016. Likewise, in Indonesia, the ITE Law does not explicitly contain the requirements stated in Article 17 of the GDPR, such as deleted data must be irrelevant, inaccurate, or obtained illegally. This specific provision is mandated by the ITE Law to be regulated in government regulations and ministerial regulations. A similar concept to RTBF is essentially the "Right to be forgotten" in Article 26 paragraphs (3) and (4) of the ITE Law. Although the right to be forgotten is not entirely similar tothe concept of RTBF because the fundamental difference that distinguishes the two is the result of fulfilling that right (Noval, 2019).

In RTBF, this information will disappear from search engine results but can still be found on the original link the data information is located. So, RTBF is often referred to as a step to make it difficult for someone to access information about someone on a search engine site results in order to respect their privacy. Privacy is vital in this fast-paced and limitless digital era. However,the concept of the right to be forgotten, applied in Indonesia, is broader than that because it deletes a person's data and deletes data from search engine site results complete with the original link to the data source. In addition, the right to be forgotten is a person's right to have information about himself deleted from cyberspace if he is found not guilty by a court in a case, so that does not mean all his personal digital information is deleted. However, the deletion of personal data also has implications for the use of personal data for general purposes. For example, information about a person proven to have committed corruption is related to disclosing information by the public interest and public funds, so it is better if the request for the deletion of such digital information cannot be granted. Therefore, the Government needs to formulate a policy direction for this right to be forgotten, not to limit other rights.

Concerning deep fakes in cyberterrorism, e-terrorism and cyber-social terrorism, this right to be forgotten can be applied to people harmed by disseminating deep fake videos by removing the link between their data and propaganda information in deep

fake videos that injure their reputation. However, this solution is reactive because it only applies if the deep fake video has spread and the video has harmed someone, for instance in cyber-social terrorism and other personal purposes such as pornographic contents. Consequently, responsive and progressive solutions are still required for law enforcement to impact deep fake technology negatively. And its legal measures are highly demanded in combating cybercriminals with high-level danger and with broad impacts such as cyberterrorism, e-terrorism and cyber-social terrorism.

Conclusion

The characteristics of deep fake that distinguish it from other video engineering methods are (1) the involvement of AI, (2) distorted data engineering through machine learning, (3) the purpose of communication is to manipulate a person's mindset through the concept of "seeing id believing," and (4) utilization for activities that violate legal norms and the rule of law. Digital personal data used in deep fake technology, regardless of consent data or non-consent data belonging to public figures and the general public, must be protected by law so that irresponsible parties do not use them. It also appears for the public interest in processing false information that is at risk of disrupting the order of people's lives.

Although deep fake technologies were first widely known from the political sphere, the various features they offer can be abused by cybercriminals by spreading various political propaganda platforms. This would imply that the application of deep fake technology by cyberterrorism is very possible. The consequence is very dangerous and severe disruption of infrastructure, by integrating various features of deep fake to disrupt established norms and institutions in political, economic and social spheres. As an implication, by reflecting on the negative effect of deep fake on politics, various measures for digital forensics, steganography methods and AI-based technical solutions can be applied to prevent and counter ideological propaganda of cyberterrorism, e-terrorism and cyber-social terrorism. In addition, strengthening the capacity of anti-terrorism agencies also needs to be strengthened by strengthening legal measures that are progressive and adaptive to digital developments.

As a practical recommendation, the findings highlight that overcoming the negative impact of deep fakes in Indonesia can be done from multiple aspects, such as socialization and government literacy to the community, development of AI-based technology that can analyze deep fakes, and strengthening regulations. The government socialization aspect should be prioritized online, as it refers to the tendency of Indonesian people to interact more on the internet. Furthermore, aspects of AI-based technology can take advantage of steganography technology. Regarding the regulatory aspect, deep fake proving is mainly at the digital forensic stage, which needs to be strengthened. The slow improvement of technology in digital forensics is one of the causes of the difficulty for the government to issue legal regulations of a technical nature to prevent the circulation of deep fake technology. In addition, it also needs to be clarified regarding the implementation of the "right to be forgotten" of the ITE Law and Anti-terrorism Law in Indonesia for victims of deep fake videos to be regulated in the form of implementing regulations for the ITE Law and Anti-terrorism Law which regulates technical matters and the arrangements must not conflict and affect the public's right to obtain information with safe digital environments.

Reference

Akhgar, B., Staniforth, A., & Bosco, F. (2014). *Cyber crime and cyber terrorism investigator's handbook*. Syngress. https://doi.org/10.1016/C2013-0-15338-X

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives, 31*(2), 211-236. https://doi.org/10.1257/jep.31.2.211

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge, MA. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Antinori, A. (2019). Terrorism and deepfake: From hybrid warfare to post-truth warfare in a hybrid world. In *ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics* (pp. 23). Academic Conferences and publishing limited.

Aufderheide, P. (2018). Media literacy: From a report of the national leadership conference on media literacy. In *Media literacy in the information age* (pp. 79-86). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781351292924-4

Azali, K. (2017). *Fake news and increased persecution in Indonesia*. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/wp-content/uploads/pdfs/ISEAS_Perspective_2017_61.pdf

Barari, S., Lucas, C., & Munger, K. (2021). Political deepfakes are as credible as other fake media and (sometimes) real media. *OSF Preprints*. https://doi.org/10.31219/osf.io/cdfh3

Barometer, E. T. (2021). *Global Report 2021*. https://www.edelman.com/trust/2021-trust-barometer

Brantly, A. F. (2018). When everything becomes intelligence: machine learning and the connected world. *Intelligence and National Security, 33*(4), 562-573. https://doi.org/10.1080/02684527.2018.1452555

Brotherton, R., French, C. C., & Pickering, A. D. (2013). Measuring belief in conspiracy theories: The generic conspiracist beliefs scale. *Frontiers in psychology*, 279. https://doi.org/10.3389/fpsyg.2013.00279

Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Elsevier Science. https://books.google.com.pk/books?id=xNjsDprqtUYC

Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Aff, 98*, 147. https://heinonline.org/HOL/LandingPage?handle=hein.journals/fora98

Crawford, K., Miltner, K., & Gray, M. L. (2014). Big Data: Critiquing Big Data: Politics, Ethics, Epistemology. *International Journal of Communication, 8*, 1663-1672. https://www.research.ed.ac.uk/en/publications/big-data-critiquing-big-data-politics-ethics-epistemology

Dawson, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. IGI Global. https://books.google.com.pk/books?id=8IQfCgAAQBAJ

De Maio, M. (2019). Argentine Media Regulation, Fake News, and the Election of Mauricio Macri. In *Oxford Research Encyclopedia of Latin American History*. https://doi.org/10.1093/acrefore/9780199366439.013.709

De Ruiter, A. (2021). The distinct wrong of deepfakes. *Philosophy & Technology, 34*(4), 1311-1332. https://doi.org/10.1007/s13347-021-00459-2

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. RAND Corporation. https://books.google.com.pk/books?id=92yRDwAAQBAJ

Fontaine, R., & Kliman, D. M. (2013). International order and global swing states. *The Washington Quarterly, 36*(1), 93-109. https://doi.org/10.1080/0163660X.2013.751653

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science advances, 5*(1), eaau4586. https://www.science.org/doi/full/10.1126/sciadv.aau4586

Hasen, R. L. (2019). Deep Fakes, Bots, and Siloed Justices: American Election Law in a'Post-Truth'World. *Louis ULJ, 64*, 535. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stlulj64

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of information technology & politics, 15*(2), 81-93. https://doi.org/10.1080/19331681.2018.1448735

Hower, S., & Uradnik, K. (2011). *Cyberterrorism*. Santa Barbara, CA: Greenwood.

Indonesia, M. T. (2019). *Results of the 2019 National Hoax Outbreak Survey*. https://mastel.id/hasil-survey-wabah-hoax-nasional-2019/

Intelligence, M. (2021). *Facial Recognition Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026)*. https://www.mordorintelligence.com/industry-reports/facial-recognition-market

Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Comparative strategy, 39*(2), 113-127. https://doi.org/10.1080/01495933.2020.1718983

Kliman, D. M. (2012). The west and global swing states. *The International Spectator, 47*(3), 53-64. https://doi.org/10.1080/03932729.2012.700017

Lai, X., & Rau, P.-L. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior, 124*, 106894. https://doi.org/10.1016/j.chb.2021.106894

Lestari, A., & Sari, D. M. (2020). Efektivitas Penerapan Undang-Undang Ite Terhadap Pelaku Penyebaran Hoaks Covid-19 Di Media Sosial. *Jurnal Transformasi Administrasi, 10*(02), 198-211. https://doi.org/10.56196/jta.v10i02.164

Levine, A. J. (2020). *Dollars, Deception, and Deepfakes: An Analysis of Deepfakes and Synthetic Media Fraud.* (Doctoral dissertation). Utica College. https://www.proquest.com/openview/3478b3271849d82d95faf5bb40d5d7b1

Microsoft. (2019). *Microsoft Security Endpoint Threat Report 2019*. https://news.microsoft.com/apac/features/microsoft-security-endpoint-threat-report-2019-asia-pacific/

Muzykant, V. L., Muqsith, M. A., Pratomo, R. R., & Barabash, V. (2021). Fake news on COVID-19 in Indonesia. In *Pandemic Communication and Resilience* (pp. 363-378). Springer. https://doi.org/10.1007/978-3-030-77344-1_22

Nastiti, F. E., Prastyanti, R. A., Taruno, R. B., & Hariyadi, D. (2018). Social media warfare in Indonesia political campaign: A survey. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)* (pp. 49-53). IEEE. https://doi.org/10.1109/ICITISEE.2018.8720959

Noval, S. M. R. (2019). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi: Penggunaan Teknik Deepfake. In *Prosiding Seminar Nasional Penelitian & Pengabdian Kepada Masyarakat 2019* (pp. 13-18). https://www.researchgate.net/profile/Sayid-Noval/publication/337830461

Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs, 74*(4), 439-454. https://doi.org/10.1080/10357718.2020.1734772

Rahmanti, A. R., Ningrum, D. N. A., Lazuardi, L., Yang, H.-C., & Li, Y.-C. J. (2021). Social media data analytics for outbreak risk communication: public attention on the "New Normal" during the COVID-19 pandemic in Indonesia. *Computer Methods and Programs in Biomedicine, 205*, 106083. https://doi.org/10.1016/j.cmpb.2021.106083

Ramanouski, V. (2019). Possible use of aI Technologies in Counterterrorism Responses by Iraqi Security establishment. In *Proceedings of the European Conference on the Impact of AI and Robotics, EM-Normandie Business School, Oxford, UK* (Vol. 31, pp. 261-265).

Sayler, K. M. (2020). *Emerging Military Technologies: Background and Issues for Congress*. Congressional Research Service. https://apps.dtic.mil/sti/pdfs/AD1105857.pdf

Schick, N. (2020). *Deepfakes: The Coming Infocalypse*. Grand Central Publishing. https://books.google.com.pk/books?id=QjndDwAAQBAJ

Susilo, S., & Dalimunthe, R. P. (2019). Moderate southeast asian islamic education as a parent culture in deradicalization: Urgencies, strategies, and challenges. *Religions, 10*(1), 45. https://doi.org/10.3390/rel10010045

Talihärm, A.-M. (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review, 3*(2), 59-74. https://www.coedat.nato.int/publication/datr/volumes/datr6.pdf#page=64

Taylor, B. C. (2021). Defending the state from digital Deceit: the reflexive securitization of deepfake. *Critical Studies in Media Communication, 38*(1), 1-17. https://doi.org/10.1080/15295036.2020.1833058

Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies–a danger for Europe? *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-06-2017-0024

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media+ Society, 6*(1). https://doi.org/10.1177/2056305120903408

Veerasamy, N. (2020). Cyberterrorism–the spectre that is the convergence of the physical and virtual worlds. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 27-52). Elsevier. https://doi.org/10.1016/B978-0-12-816203-3.00002-2

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11). https://timreview.ca/article/1282

Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy, 5*(2), 199-217. https://doi.org/10.1080/23738871.2020.1797135

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. Library of Congress Washington Dc Congressional Research Service. https://apps.dtic.mil/sti/citations/ADA477642

Wolman, D. (2013). *The End of Money: Counterfeiters, Preachers, Techies, Dreamers--and the Coming Cashless Society*. Hachette UK. https://lib.hpu.edu.vn/handle/123456789/28827

Yerlikaya, T., & Aslan, S. T. (2020). Social Media and Fake News in the Post-Truth Era. *Insight Turkey, 22*(2), 177-196. https://www.jstor.org/stable/26918129

Yu, S., & Carroll, F. (2021). Implications of AI in National Security: Understanding the Security issues and Ethical challenges. In *Artificial Intelligence in Cyber Security: Impact and Implications* (pp. 157-175). Springer. https://doi.org/10.1007/978-3-030-88040-8_6