SRIWIJAYA CRIMEN AND LEGAL STUDIES
FACULTY OF LAW UNIVERSITAS SRIWIJAYA
Jalan Srijaya Negara, Palembang, 30139, Indonesia
Email: scls@fh.unsri.ac.id
http://journal.fh.unsri.ac.id/index.php/SCLS/index
E-ISSN: 2987-7350 P-ISSN: 2986-6367

DEEPFAKE IN ONLINE FRAUD CASES: THE HAZE OF ARTIFICIAL INTELLIGENCE'S ACCOUNTABILITY BASED ON THE INTERNATIONAL LAW

Orima Melati Davey[1], Levin Sauerwein[2]

[1]*International Tribunal for the Law of the Sea, Germany, E-mail: orimadavey23@gmail.com*
[2]*Business Psychology HAM, Germany, E-mail: levinsauerwein77@googlemail.com*

Article

Keywords:
Accountability, Artificial Intelligence, Deepfake, Online Loans.

DOI:
10.28946/scls.v1i2.2654

Abstract

Artificial Intelligence (AI) is the science and engineering of intelligent machines, primarily through computer programs. AI consists of processes by human intelligence simulated through machine processes and is concerned with designing, developing, and implementing computer systems. One of them is Deepfake. Deepfake is a technology that uses data as an image/photo of a person's face, which is part of personal data and potentially misused to commit crimes such as online loan fraud. The research discusses (1) the Benefits and Disadvantages of Artificial Intelligence in Human Lives, (2) the concept of accountability for deepfake artificial intelligence in online loan fraud according to international law and its application in Indonesia, and (3) the analysis of regulations and accountability of deepfake according to chaos theory. The research uses a legal-normative approach. Moreover, the research will examine legal principles, systematics, and comparative law in its application. The research illustrates that deepfake accountability as artificial intelligence in online loan fraud according to international law is described in the General Recommendation on the Ethics of Artificial Intelligence by The United Nations Educational, Scientific, and Cultural Organization (UNESCO). Meanwhile, the concept of accountability in Indonesia is seen in Human Rights and Data Privacy Violations. According to chaos theory, the analysis of Deepfake's regulatory and accountability concept in international and national law leads to inconsistencies because it is only a recommendation, yet to be integrated, and still multidimensional.

A. INTRODUCTION

Artificial Intelligence (AI) is a general term that uses computers as a model of intelligent behavior with minimal human intervention.[1] From another perspective, Artificial Intelligence is seen as the ability of devices to carry out activities that should only be expected from human intelligence.[2] Artificial intelligence is the oldest and broadest field of computer science, and it is related to all aspects that mimic cognitive functions in problem-solving, building learning systems, and thinking like humans.[3] Artificial intelligence is rapidly adopted in many industries to increase performance, precision, and time efficiency and reduce costs.[4] John McCarthy created the term artificial intelligence, an experimental branch of computer science that aims to create intelligent machines that perform various tasks using their intelligence.[5] This development has led some to suggest that humanity is in the fourth industrial revolution, in which technology blurs the boundaries between the physical, digital, and biological realms.[6]

AI is predicted to become available, namely, machines that can approach human abilities in various things such as thinking, communicating in languages that humans and machines understand, reasoning, planning, etc. The benefit of AI is developing methods and systems to solve a problem that humans can solve. For example, search for places, businesses, and households and improve the performance of computer-based information systems.

One of the more popular AI is deepfake. Besides a large number of personal data sales and the creation of simulated data via the internet, it turns out that the personal data of online loan victims is also obtained in various ways, especially for those who are still not careful about using their data. For example, using phishing methods, namely using fake websites that duplicate the original website so that people who are not careful can be fooled into entering/registering their personal information/data, or when applying for a job, the murder victim scans/photocopies their ID Card, Family Card, or diploma on the Curriculum Vitae (CV) which should not have been provided even though requested—even sending a photo of the ID Card when installing applications that claim to get a bonus balance if registering a picture of the ID Card. These data are likely to be misused by unauthorized people.

Suppose this data is used to register a loan online. In that case, the perpetrator asks for a photo of himself holding the ID Card or a selfie, so this artificial intelligence technology deepfake is needed. The perpetrator only needs to take a picture of himself (selfie) while holding the ID Card. From the photo results, the deepfake changes the perpetrator's face to the victim's face, and the image of the perpetrator's ID Card is changed to become the victim's ID Card or the data on the ID Card is changed to data belonging to the victim. After getting a photo of someone else's ID Card, the perpetrator efficiently used the personal data for advantage.[7] In this case, the perpetrator has detained someone's data or information and misused it for profit. The

[1] Pavel Hamet and Johanne Tremblay, "Artificial Intelligence in Medicine," *Metabolism: Clinical and Experimental* 69 (2017): S36–40, https://doi.org/10.1016/j.metabol.2017.01.011.
[2] Deloitte and Efma, "AI and You: Perceptions of Artificial Intelligence from the EMEA Financial Services Industry," *Deloitte* (Milan, 2017).
[3] Andreas Holzinger et al., "Causability and Explainability of Artificial Intelligence in Medicine," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 9, no. 4 (2019): 1–13, https://doi.org/10.1002/widm.1312.
[4] Yoav Mintz and Ronit Brodie, "Introduction to Artificial Intelligence in Medicine," *Minimally Invasive Therapy and Allied Technologies* 28, no. 2 (2019): 73–81, https://doi.org/10.1080/13645706.2019.1575882.
[5] A. Yadav et al., "Artificial Intelligence - New Era," *International Journal of New Technology and Research* 3, no. 3 (2017): 263339.
[6] Klaus Schwab, *The Fourth Industrial Revolution* (New York: Crown Publishing Group, 2017), 64.
[7] Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, "Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake," *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 01 (2022): 25–39, https://doi.org/10.24123/YUSTIKA.V25I01.5091.

existence of a fake photo using a deepfake made by the perpetrator can make it difficult for the victim to clearly show evidence that he has never applied for a loan.

Deepfake technology uses data in the form of images/photos of a person's face, which part of personal data potentially misused to commit crimes such as pornography, revenge, bullying, political sabotage, extortion, fake video evidence, fraud, identity theft, and privacy issues other. The perpetrator is forging someone's data using deepfake technology to gain profit, resulting in losses for the victim. The leakage of personal data through terror threats by debt collectors will spread the victim's data. If he does not pay off the debt and material losses in the amount of money obtained by the perpetrator using the victim's data on online loan services, even though the victim did not receive the loan.[8] The novelty of this research is the accountability of frauds using deepfake as a form of artificial intelligence using the chaos theory analysis based on international law. Based on this background description, the research will discuss (1) How is the concept of deepfake accountability as artificial intelligence in online loan fraud according to international law and the application in Indonesia? (2) How is deepfake's regulatory and accountability analysis according to chaos theory?

B. RESEARCH METHOD

This research uses a normative legal research method. The research will examine legal principles, systematics, and comparative law in its application. Based on the nature of the research, it describes the data in detail to find facts, identify problems, and discuss issues. Sources of data used in research are secondary data sources. In this particular legal research, secondary data is categorized into three legal materials: primary legal materials, secondary legal materials, and tertiary legal materials.

C. ANALYSIS AND DISCUSSION

1. Benefits and Disadvantages of Artificial Intelligence in Human Lives

In economics and finance, AI helps in various matters such as financial investments, financial records, buying and selling shares, fraud, and bank criminalization. In aviation, AI is used to simulate flights so that pilots can be assisted by providing the best movement information, air condition, pressure information, etc. Although this is not widely practiced, robotic tutors have been introduced to teach children everything from biology to computer science. Machine learning in AI is used to assess what needs to be improved for each student in the learning process. In the industrial sector, robots are often found to replace humans, especially in repetitive jobs, such as automatic machines in factories that help produce a product.[9]

Artificial intelligence has been proven to provide advantages in human lives. AI automates repeated learning and discovery through data. But AI is different from hardware-driven robotic automation. Instead of automating manual tasks, AI performs frequent, high-volume, computerized duties reliably and without fatigue. Human inquiry is still essential for this automation to set up the system and ask the right questions. AI adds intelligence to existing products.

In most cases, AI is not sold as an individual application. However, products you already use will be enhanced with AI capabilities, like Siri being added as a feature to a new generation of Apple products. Automation, conversational platforms, bots, and intelligent machines can be

[8] Hafsah Amalia Afnan and wardah Yuspin, "Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online," *Universitas Muhammadiyah Surakarta.*, March 17, 2022, http://eprints.ums.ac.id/99046/.
[9] BARKI, "Manfaat Kecerdasan Buatan Bagi Kehidupan Manusia," Universitas Medan Area, 2022.

combined with massive amounts of data to enhance many technologies in the home and workplace, from security intelligence to investment analysis. AI adapts through progressive learning algorithms to enable data to do programming. AI finds structure and order in data, so the algorithm gains skill: The algorithm becomes a classifier or predictor. So, just as an algorithm can teach how to play chess, AI can teach itself what product to recommend online. And models adapt as they provide new data. Back propagation is an AI technique that allows a model to adjust through training and added data when the first answer is incorrect.

Everything is changing with the incredible power of computers and big data. AI analyzes data deeply by using neural networks with many hidden layers. Building a fraud detection system with five hidden layers was nearly impossible a few years ago. It would be best to have a lot of data to train deep learning models because the models learn directly from the data. The more data you feed to the model, the more accurate it will be. AI achieves astonishing accuracy through deep neural networks, which was impossible before. For example, your interactions with Alexa, Google Search, and Google Photos are all based on deep learning, and they continue to become more accurate as we use them more and more. In the medical field, AI techniques from deep learning, image classification, and object recognition can now be used to find cancer on MRI with the same accuracy as trained radiologists. The answer is in the data; You need to apply AI to get them. AI utilizes most of the data. If the algorithm is self-learning, the data becomes intellectual property. The role of data is now more critical than ever. It creates a competitive advantage. If you have the best data in a competitive industry, even if someone applies a similar technique, the best data will win.[10]

The negative impacts will arise in employees in several fields, including transaction activity, reduction of goods' process production, and analysis.[11] In addition, there are other effects, such as:[12]

1. Privacy violation
   Privacy violation is concerning in AI utilization because everyone who accesses the internet will disclose their data or information into the digital world. Afterward, the data and information will be neatly stored in big data.[13] Big data then involves the analysis of artificial intelligence, which functions to find correlations and is then used to inform decisions that affect individuals. It can potentially cause privacy problems and other problems that are even broader.[14]

2. Deepfake
   Deepfake is a technique for synthesizing human images based on artificial intelligence, in which an image or video can be combined with specific methods to make the results appear natural.[15] Artificial Intelligence Deepfake is a technology that can help humans work. Still, this technology could be misused by certain parties so that it can harm other people, such as through forgery and misuse of personal data to get online loans.[16]

---

[10] SAS, "Mengapa Kecerdasan Buatan Penting?," 2022.
[11] John Chelliah, "Will Artificial Intelligence Usurp White Collar Jobs?," *Human Resource Management International Digest* 25, no. 3 (2017): 1–3, https://doi.org/10.1108/HRMID-11-2016-0152.
[12] Muhammad Yusril Rian Soares, "5 Dampak Buruk Perkembangan AI," Universitas Alma Ata, 2021.
[13] Zaid, "Ketika Keamanan Privasi Data Pribadi Semakin Rentan, Bagaimana Negara Seharusnya Berperan?," *Volksgeist* 4, no. 1 (2021): 25–37, https://doi.org/10.24090/volksgeist.v4i1.4492.
[14] Moira Paterson and Maeve McDonagh, "Data Protection in an Era of Big Data: The Challenges Posed By Big Personal Data," *Monash University Law Review* 44, no. 1 (2018): 1–31.
[15] Heny Novyanti and Pudji Astuti, "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana," *Novum: Jurnal Hukum* 1, no. 1 (2021): 1–18, https://doi.org/10.2674/novum.v0i0.43571.
[16] Hafsha Amalia Afnan, "Perlindungan Hukum Penyalahgunaan Artificial Intellegence Deepfake Pada Layanan Pinjaman Online" (Universitas Muhammadiyah Surakarta, 2022).

3. Weapon automation
   AI is a technological innovation that can become a deadly weapon and threaten the security of a country.[17] One example of using AI as weapon automation is the Lethal Autonomous Weapon System (LAWS). LAWS, or lethal autonomous weapons, are a type of autonomous military robot that can independently search for and engage targets based on programmed boundaries and descriptions.[18] Deadly autonomous weapons present new legal, ethical, moral, and strategic challenges. This further increases the awareness and discussion of the world community about the possibility of lethal autonomous weapons systems in the future that can change the human relationship with violence in war.[19]

2. The Concept of Deepfake Accountability as Artificial Intelligence in Online Loan Fraud According to International Law and Its Application in Indonesia

Information technology in the digital era is developing rapidly and influences many sectors, including the economy. Technological developments, computer systems, and the internet have also resulted in the transmission of information and data quickly and easily being stored, searched, and shared. Various activities initially carried out by interacting directly with other people or visiting specific sites can now be done without going to that place or through the internet (online) using a smartphone or computer. This situation is a loophole for deepfake crimes.

a. The Concept of Accountability for Deepfake as Artificial Intelligence According to International Law

In November 2021, the United Nations Educational, Scientific and Cultural Organization (UNESCO) established a Recommendation on the Ethics of Artificial Intelligence. The recommendations contain the principles and standards complied with in the legal framework of member countries regarding the use of AI.[20] The recommendations state that AI Actors and Member States should respect, protect, and promote human rights and fundamental freedoms, promote the protection of the environment and ecosystems, assuming their respective ethical and legal responsibilities following national and international law, in particular Member States' human rights obligations, and ethical guidance throughout the lifecycle of an AI system, including concerning AI actors within their effective area and control. Ethical responsibilities and obligations for decisions and actions based on AI systems in any way must ultimately be attributed to AI actors appropriate to their role in the AI system life cycle.

Besides UNESCO, the European Commission has a Liability Directive, namely the Liability Directive.[21] The AI Liability Directive aims to establish unity rules for access to information, reduce the burden of proof concerning damages caused by AI systems, establish broader protections for victims (individuals or businesses), and encourage the AI sector by increasing

[17] Donovan Typhano Rachmadie and Supanto, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016," *Recidive* 9, no. 2 (2020): 128–36.
[18] Rebecca Crootof, "The Killer Robots Are Here: Legal and Policy Implications," *Cordozo Law Review* 36, no. 5 (2015): 1837–1915.
[19] Ryan Muhammad Fahd and Bambang dwi Waluyo, "Telaah Konstruktivis Partisipasi Cina Dalam the Campaign to Stop Killer Robots," *Indonesian Journal of International Relations* 4, no. 2 (2020): 92–113, https://doi.org/10.32787/ijir.v4i2.123.
[20] Mark Ryan and Bernd Carsten Stahl, "Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications," *Journal of Information, Communication, and Ethics in Society* 19, no. 1 (2021): 61–86, https://doi.org/10.1108/JICES-12-2019-0138/FULL/PDF.
[21] Anthony Wong, "Ethics and Regulation of Artificial Intelligence," *IFIP Advances in Information and Communication Technology* 614 (2021): 1–18, https://doi.org/10.1007/978-3-030-80847-1_1/COVER.

underwriting.[22] The European Commission adopted two proposals to adapt accountability rules to the digital age, circular economy, and global value chain impacts. First, it proposes modernizing the rules on manufacturers' strict accountability for defective products (from smart technology to pharmaceuticals). The revised rules will give businesses legal certainty to invest in new and innovative products and ensure that victims receive fair compensation when defective products, including digital and refurbished products, incur losses. Second, the Commission proposes harmonizing national accounting rules targeted for AI for the first time.[23] So, it is easier for harmed AI victims to receive compensation. In line with the goals of the AI White Paper and with the AI Commission's 2021 proposal, establishing a framework for excellence and trust in AI, the new rules will ensure that victims benefit from the same standard of protection when harmed by an AI product or service, as they would if the harm was caused under other circumstances.

b. Accountability of Deepfake as Artificial Intelligence in Online Loan Fraud in Indonesia

According to the principle of accountability in criminal law, a crime is not committed if there is no mistake (*Geen straf zonder schuld; Actus non facit reum nisi mens sir rea*). AI's accountability focuses on accountability for the crimes committed because of one's actions. It should be noted that private persons (Naturalijk Persoon) who are the subject of criminal law in Indonesia are the subject of the country's primary criminal law. However, in line with the expansion of this subject, legal entities (corporations) can also become subjects of criminal law in Indonesia.[24] Interpretation is needed to determine whether artificial intelligence (AI) is legal in Indonesia because no specific regulations govern it.

According to Law No. 19 of 2016 concerning Information and Electronic Transactions, AI is an electronic system and electronic agent, so all actions carried out by AI must first obtain permission from humans. According to the ITE Law, authorization is granted by electronic system operators, which covers many legal subjects.[25] Since criminal accountability is one of the independent skills owned by legal subjects, and because AI only has automatic conditions created by humans, it has no independent skills. Therefore, AI cannot be said to separate legal matters or be equivalent to other legal subjects. Furthermore, protection of personal data is the right of every person to maintain the confidentiality of personal data as stipulated in Article 26 paragraphs (1) and (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which states that:[26]

(1) "Unless otherwise stipulated by laws and regulations, the use of any information through electronic media concerning personal data must be carried out with the consent of the person concerned."
(2) "Every person whose rights are violated as referred to in paragraph (1) can file a lawsuit for losses incurred under this Law."

[22] Caroline Cauffman, "Robo-Liability: The European Union in Search of the Best Way to Deal with Liability for Damage Caused by Artificial Intelligence," *Https://Doi.Org/10.1177/1023263X18812333* 25, no. 5 (2018): 527–32, https://doi.org/10.1177/1023263X18812333.
[23] European Commission, "New Liability Rules on Products and AI to Protect Consumers and Foster Innovation," 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.
[24] Muhammad Tan Abdul Rahman Haris and Tantimin Tantimin, "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 307–16, https://doi.org/10.23887/JKH.V8I1.44408.
[25] Rachmadie and Supanto, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016."
[26] Hwian Christianto, "Konsep Hak Untuk Dilupakan Sebagai Pemenuhan Hak Korban Revenge Porn Berdasarkan Pasal 26 Undang-Undang Informasi Dan Transaksi Elektronik," *Mimbar Hukum : Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada* 32, no. 2 (2020): 175, https://doi.org/10.22146/JMH.51110.

Everyone has the right as the owner of personal data always to maintain the confidentiality of personal data based on the provisions of Article 26 paragraphs (1) and (2). If personal data is misused or shared widely by other parties, then the owner whose data is misused can file a lawsuit—civil law accompanied by compensation to court.

The progress of the internet system and the ease of exchanging data is increasingly massive, which causes the vulnerability to interference with personal data privacy. A person's data becomes easy to distribute arbitrarily to spaces accessed by the public without the knowledge and permission of the data owner. Therefore, it is necessary to regulate the protection of personal data. Protection of privacy and personal data is stated in the 1945 Constitution of the Republic of Indonesia (1945 Constitution) Article 28G, which stipulates that everyone has the right to protection of themselves, their family, honor, dignity, and property under their control, and the right to feel safety and protection from the threat of fear to do or not do something as a human right.[27]

Personal, family, honor, dignity, and property rights. Provisions for the protection of personal data in the 1945 Constitution are a mandate given directly by the Constitution of the Republic of Indonesia, which contains respect for human rights values, so it needs to be given a legal basis to provide more protection and security of personal data which then spread in various laws. In general, one of the laws that have rules related to the protection of personal data is Law Number 39 of 1999 concerning Human Rights, namely in Article 29 Paragraph (1) and Article 32, which stipulates that everyone has the right to self-protection.[28] In addition, it is also regulated that independence and confidentiality in correspondence, including communications through electronic means, cannot be disturbed.

A series of actions by perpetrators who falsified the victim's data using deepfake technology are included in activities that are prohibited by law as stated in Article 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008: "Every person intentionally and without rights or against the law to manipulate, create, change, delete, destroy Electronic Information and Electronic Documents with the aim that the Electronic Information and Electronic Documents are considered as if they were authentic data. Violation of this Article is punishable by a maximum imprisonment of 12 (twelve) years and a maximum fine of Rp. 12,000,000,000.00 (twelve billion rupiahs).

Although a series of counterfeiting acts committed by perpetrators using deepfake technology has not been regulated explicitly through laws and regulations, it is based on the provisions stipulated in Article 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. It links acts of forgery committed by perpetrators with guarantees of legal certainty for victims of personal data falsification using deepfake technology.[29] Such protection is the right of victims to protect their personal data/information from alteration or destruction so that the manipulated data/information is considered original and authentic data whether used for any purpose. If the rights owned are violated, the victim can resolve the problem through legal remedies by filing a lawsuit with the court. Filing a lawsuit in court is not only to prosecute the perpetrators of falsifying the victim's data by using deepfake technology but also against online loan

[27] Pembaharuan Hukum et al., "Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)," *Jurnal Hukum Mimbar Justitia* 8, no. 1 (2022): 233–53, https://doi.org/10.35194/JHMJ.V8I1.2426.

[28] Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99, https://doi.org/10.25072/JWY.V5I2.460.

[29] Parlin Doni Sipayung, "Tinjauan Yuridis Tindak Pidana Penyebaran Kebencian Melalui Media Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus Putusan Nomor: 572/Pid.B/2016/Pn.Jkt.Sel)," *Jurnal Ilmiah Maksitek* 3, no. 4 (2018).

providers who have disseminated the victim's data through billing terror as well as other parties who have no legal relationship with the owner of the personal data who has disseminated the victim's data. Legal action against the court is filed to recover the situation and return the losses suffered.

Provisions contained in laws and regulations governing the protection of personal data in general, such as the 1945 Constitution, Law no. 39 of 1999 concerning Human Rights, and Law no. 19 of 2016 concerning ITE, it turns out that none of them have regulated or merely alluded to the misuse and falsification of personal data using AI deepfake technology. The laws and regulations only state that the right to personal data protection is everyone's right, the obligation to maintain the confidentiality of personal data, or the need to obtain permission from the owner of personal data before using it. These laws and regulations do not explain if personal data, as the right of every person, is misused in specific ways, namely using AI deepfake technology, such as in cases of personal data forgery using AI deepfake to get online loans.[30] Even though deepfake technology is prevalent for use in the digital era, it causes many losses and violates the victim's data protection rights.

3. Analysis of Deepfake Regulations and Accountability According to Chaos Theory

Based on the concept of deepfake accountability under international laws and regulations, research has yet to see the effectiveness of the concept. According to chaos theory, accountability in the international and national areas has yet to be complementary, leading to disorders. Chaos denotes disorder, randomness, or chance, that is, random movement without any particular purpose, purpose, or principle. This dynamic universe seems to work through a linear system, but many things do not work linearly and cannot be understood through a linear system, such as clouds, trees, coastlines, waves, and so on, which at first glance appear random and irregular. Systems like this are called chaos theory, a theory related to natural processes that seem chaotic, spontaneous, and non-linear (systems that cannot be predicted based on initial conditions).

Chaos theory explains a system's complex and unpredictable movement or dynamics depending on its initial conditions. Even though it occurs randomly, the chaotic system can be determined mathematically. This is because the chaotic system follows the laws that apply in nature.[31] Chaos Theory is a theory that explains complex and unpredictable changes or dynamic systems that are sensitive to initial conditions. It's just that because of its fickle nature, it is seen as a random event. Chaotic can be found in various general systems, ranging from simple techniques such as precursors to complex systems such as the rhythm of the heartbeat, electrical activity in the brain, and so on. Economic systems such as price movements on the stock exchange, currency exchange rates, and crude oil prices are chaotic.[32] The chaos system is mathematically deterministic (as opposed to probabilistic). It follows precise laws, but its disorderly behavior can appear random to the casual observer.

The spectrum of behavior for compliance with international legal norms ranges from fully accepted cooperation to some forms of coercion. At some point in this range is consensus, a type of agreement that satisfies one party's goals in part to fully satisfy another party's achievement of acceptance of a norm. Many of the law-making instruments witnessed in the past have emerged from international organizations, particularly the United Nations. However, even if

[30] Sophie Maddocks, "'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities between Pornographic and 'Political' Deep Fakes," *Journal of Artificial Studies and Policies* 7, no. 4 (2020): 415–23, https://doi.org/10.1080/23268743.2020.1757499.

[31] Dian Purworini, Dini Purnamasari, and Desi Puji Hartuti, "Crisis Communication in a Natural Disaster: A Chaos Theory Approach," *Jurnal Komunikasi: Malaysian Journal of Communication* 35, no. 2 (2019): 2019, https://doi.org/10.17576/JKMJC-2019-3502-03.

[32] shahtaj Shaukat et al., "Chaos Theory and Its Application: An Essential Framework for Image Encryption," *Chaos Theory and Applications* 2, no. 1 (2020): 17–22.

non-cooperation is rooted in a loss of state ability and willingness to cooperate, laws can set incentives that encourage state (and other actors) disaster prevention behavior.

International law may not be an automatic solution to eliminating chaotic conditions or frequent armed conflicts. However, international law certainly does not advocate, promote, or propose policies that support the requirements that seek to destroy. By its very nature, international law operates in a world with states interacting at many intersections of interests that can be adapted to a set of norms in the reverse order of serious benefit on coercive, negotiated, mutual, or evolutionary grounds. Consensus development does not always depend on the implicit agreement but occurs only as the simultaneous emergence of self-interest appreciation. However, there should be no hope of reducing the conflict.

On the other hand, the dislocation of the civil order beyond state boundaries can only be achieved. As the description above, a level of hope that secures a goal at least in maximum losses level.[33] Regarding the deepfake case, international legal accountability still needs to be clarified in providing a settlement because there are no binding or integrated regulations discussing AI.

In constitutional law, chaos theory in the legal system does not imply inconsistencies or conflicts between the sub/sections in the system. If there is an inconsistency between subsections and the overall system, this is called a "sick system". However, because the law is a "sound system", if there is an inconsistency, there is already a mechanism for resolving the inconsistency. The mechanisms for overcoming these inconsistencies are: 1) application of statutory principles, namely (a) the highest law overrides the lower law, (b) the current law overrides the former law; 2) examination of laws, both formal and material; 3) revisions or changes made by the former (legislative review); 4) interpretation by judges or state administration bodies; (5) legal construction carried out by judges which can be in the form of analogies and legal elaborations. Although the law is an orderly system and mechanism for dealing with inconsistencies, there are also aspects of the law's irregularity. Thus, anomalies occur in acts not under the law, or they feel they act according to their rights and obligations according to their respective perceptions. Examples of these forms of disorder in Indonesia can be in the form of behavior or attitudes towards mass violence, land plots without rights, fencing or blocking of toll roads and main roads, occupation of the district head's office, and so on. Research needs to be more consistent in deepfake accountability in Indonesia, which is neither comprehensive nor integrated because they have to look at various aspects (multidimensional).

D. CONCLUSION

The concept of deepfake accountability as artificial intelligence in online loan fraud according to international law is generally described in the Recommendation on the Ethics of Artificial Intelligence by UNESCO. The accountability is adjusted to the ethics and law of each, following national and international law, especially human rights obligations. Meanwhile, the concept of accountability in Indonesia is seen in Human Rights and Data Privacy Violations. This provision is regulated in the 1945 Constitution, Law No. 39 of 2016 concerning Human Rights, and Law No. 19 of 2016 concerning Information and Electronic Transactions.

According to chaos theory, deepfake regulatory and accountability analysis is that the concept of accountability in international law can lead to inconsistencies because it is only a recommendation, and there needs to be integrated regulations related to AI accountability. Meanwhile, in the Indonesian legal system, inconsistencies in accountability are seen in multidimensional and non-comprehensive regulations.

[33] Sanford R Silverburg and Shadi Alshdaifat, "Saudi Journal of Humanities and Social Sciences 'Strategic Chaos': The Role of International Law," accessed December 17, 2022, https://doi.org/10.21276/sjhss.

REFERENCES

Afnan, Hafsah Amalia, and wardah Yuspin. "Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online." *Universitas Muhammadiyah Surakarta.*, March 17, 2022. http://eprints.ums.ac.id/99046/.

Afnan, Hafsha Amalia. "Perlindungan Hukum Penyalahgunaan Artificial Intellegence Deepfake Pada Layanan Pinjaman Online." Universitas Muhammadiyah Surakarta, 2022.

Algamar, Muhammad Deckri, and Aliya Ilysia Irfana Ampri. "Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake." *Jurnal Yustika: Media Hukum Dan Keadilan* 25, no. 1 (2022): 25–39. https://doi.org/10.24123/YUSTIKA.V25I01.5091.

BARKI. "Manfaat Kecerdasan Buatan Bagi Kehidupan Manusia." Universitas Medan Area, 2022.

Cauffman, Caroline. "Robo-Liability: The European Union in Search of the Best Way to Deal with Liability for Damage Caused by Artificial Intelligence." *Https://Doi.Org/10.1177/1023263X18812333* 25, no. 5 (2018): 527–32. https://doi.org/10.1177/1023263X18812333.

Chelliah, John. "Will Artificial Intelligence Usurp White Collar Jobs?" *Human Resource Management International Digest* 25, no. 3 (2017): 1–3. https://doi.org/10.1108/HRMID-11-2016-0152.

Christianto, Hwian. "Konsep Hak Untuk Dilupakan Sebagai Pemenuhan Hak Korban Revenge Porn Berdasarkan Pasal 26 Undang-Undang Informasi Dan Transaksi Elektronik." *Mimbar Hukum : Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada* 32, no. 2 (2020): 175. https://doi.org/10.22146/JMH.51110.

Crootof, Rebecca. "The Killer Robots Are Here: Legal and Policy Implications." *Cordozo Law Review* 36, no. 5 (2015): 1837–1915.

Deloitte, and Efma. "AI and You: Perceptions of Artificial Intelligence from the EMEA Financial Services Industry." *Deloitte*. Milan, 2017.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. https://doi.org/10.25072/JWY.V5I2.460.

European Commission. "New Liability Rules on Products and AI to Protect Consumers and Foster Innovation," 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.

Fahd, Ryan Muhammad, and Bambang dwi Waluyo. "Telaah Konstruktivis Partisipasi Cina Dalam the Campaign to Stop Killer Robots." *Indonesian Journal of International Relations* 4, no. 2 (2020): 92–113. https://doi.org/10.32787/ijir.v4i2.123.

Hamet, Pavel, and Johanne Tremblay. "Artificial Intelligence in Medicine." *Metabolism: Clinical and Experimental* 69 (2017): 36–40. https://doi.org/10.1016/j.metabol.2017.01.011.

Haris, Muhammad Tan Abdul Rahman, and Tantimin Tantimin. "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 307–16. https://doi.org/10.23887/JKH.V8I1.44408.

Holzinger, Andreas, Georg Langs, Helmut Denk, Kurt Zatloukal, and Heimo Müller. "Causability and Explainability of Artificial Intelligence in Medicine." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 9, no. 4 (2019): 1–13. https://doi.org/10.1002/widm.1312.

Hukum, Pembaharuan, Nasional Dalam, Upaya Perlindungan, Data Pribadi Di, Era Distrupsi, Kecerdasan Buatan, Abdul Hadi, and Bima Guntara. "Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)." *Jurnal Hukum Mimbar Justitia* 8, no. 1 (June 30, 2022): 233–53.

https://doi.org/10.35194/JHMJ.V8I1.2426.

Maddocks, Sophie. "'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities between Pornographic and 'Political' Deep Fakes." *Journal of Artificial Studies and Policies* 7, no. 4 (2020): 415–23. https://doi.org/10.1080/23268743.2020.1757499.

Mintz, Yoav, and Ronit Brodie. "Introduction to Artificial Intelligence in Medicine." *Minimally Invasive Therapy and Allied Technologies* 28, no. 2 (2019): 73–81. https://doi.org/10.1080/13645706.2019.1575882.

Novyanti, Heny, and Pudji Astuti. "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana." *Novum: Jurnal Hukum* 1, no. 1 (2021): 1–18. https://doi.org/10.2674/novum.v0i0.43571.

Paterson, Moira, and Maeve McDonagh. "Data Protection in an Era of Big Data: The Challenges Posed By Big Personal Data." *Monash University Law Review* 44, no. 1 (2018): 1–31.

Purworini, Dian, Dini Purnamasari, and Desi Puji Hartuti. "Crisis Communication in a Natural Disaster: A Chaos Theory Approach." *Jurnal Komunikasi: Malaysian Journal of Communication* 35, no. 2 (June 30, 2019): 2019. https://doi.org/10.17576/JKMJC-2019-3502-03.

Rachmadie, Donovan Typhano, and Supanto. "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016." *Recidive* 9, no. 2 (2020): 128–36.

Ryan, Mark, and Bernd Carsten Stahl. "Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications." *Journal of Information, Communication, and Ethics in Society* 19, no. 1 (March 3, 2021): 61–86. https://doi.org/10.1108/JICES-12-2019-0138/FULL/PDF.

SAS. "Mengapa Kecerdasan Buatan Penting?," 2022.

Schwab, Klaus. *The Fourth Industrial Revolution*. New York: Crown Publishing Group, 2017.

Shaukat, shahtaj, Arshid Ali, Amna Eleyan, Syed Aziz Shah, and Jawad Ahmad. "Chaos Theory and Its Application: An Essential Framework for Image Encryption." *Chaos Theory and Applications* 2, no. 1 (2020): 17–22.

Silverburg, Sanford R, and Shadi Alshdaifat. "Saudi Journal of Humanities and Social Sciences 'Strategic Chaos': The Role of International Law." Accessed December 17, 2022. https://doi.org/10.21276/sjhss.

Sipayung, Parlin Doni. "Tinjauan Yuridis Tindak Pidana Penyebaran Kebencian Melalui Media Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus Putusan Nomor: 572/Pid.B/2016/Pn.Jkt.Sel)." *Jurnal Ilmiah Maksitek* 3, no. 4 (2018).

Soares, Muhammad Yusril Rian. "5 Dampak Buruk Perkembangan AI." Universitas Alma Ata, 2021.

Syarifudin, Amir, and Indah Febriani. "Sistem Hukum Dan Teori Hukum Chaos." *Hasanuddin Law Review* 1, no. 2 (2018): 296–306. https://doi.org/10.20956/HALREV.V1I2.85.

Wong, Anthony. "Ethics and Regulation of Artificial Intelligence." *IFIP Advances in Information and Communication Technology* 614 (2021): 1–18. https://doi.org/10.1007/978-3-030-80847-1_1/COVER.

Yadav, A., V. Gupta, H. Sahu, and S. Shrimal. "Artificial Intelligence - New Era." *International Journal of New Technology and Research* 3, no. 3 (2017): 263339.

Zaid. "Ketika Keamanan Privasi Data Pribadi Semakin Rentan, Bagaimana Negara Seharusnya Berperan?" *Volksgeist* 4, no. 1 (2021): 25–37. https://doi.org/10.24090/volksgeist.v4i1.4492.