John Peck

24SEP2023

CYSE 201S

Prof. Duvall

Article Review - "Victimization by Deepfake in the Metaverse: Building a Practical Management Framework"

Introduction

The article that I read was "Victimization by Deepfake in the Metaverse: Building a Practical Management Framework" by Julia Stavola, M.S., and Kyung-Shick Choi, Ph.D., from Boston University, U.S.A. Both of these individuals talk about a comprehensive challenge posed by deepfake technology in the emerging metaverse. The study dives into the field of social sciences by addressing issues related to cybersecurity, human behavior, and impact of technology on society.

Social Science Principles

The article relates to several principles of social sciences. The first principle that I noticed was human behavior and cognition in the face of technological advancements. It looks into how people interact with and respond to deepfake content in the metaverse, showing the psychological and sociological aspects of human behavior. Secondly, this study aligns with the principle of ethics and social responsibility. It discusses the possible harm and ethical concerns with deepfake technology. Finally, the article looks back into interdisciplinary research by combining insights from technology, psychology, and sociology to address the issue of deepfake technology.

Research Questions and Hypotheses

The research questions and hypotheses are well thought out in this article. The authors investigate the frequency of deepfake victimization in the metaverse and its impact on humans. They also hypothesize that individuals with higher digital literacy and awareness are less likely to fall victim to deepface-related attacks. These research questions and hypotheses drive the study's investigation.

Research Methods

The article conducts a mixed-methods approach, utilizing both qualitative and quantitative research methods. Qualitative methods included interviews and surveys to gather in-depth insights into victims experiences and perceptions. Quantitative methods involved data analysis to create a baseline statistical relationship between variables. This methodological diversity enhances the in-depthness of the study.

Types of Data and Analysis

The data collected consists of qualitative responses from interviews and quantitative data from surveys. Thematic analysis is used to extract themes and patterns from the qualitative data, while the statistical analysis is used to quantitative data to test hypotheses. The combination of these data types and analyses provides an in depth perspective on the deep fake victimization phenomenon.

Concepts from Class

The article relates to concepts discussed in class, such as the cyber precipitation concept. I believe we talked about deep fakes in class, it might have not been a part of the lecture, and human behavior in online environments. It highlights the critical role of having more

digital literacy in mitigating the risks of deep fake victimization which relates to cyber precipitation, and shows the importance of understanding user behavior in the metaverse.

Challenges and Concerns of Marginalized Groups

While the article focuses on deepfake victimization, it indirectly relates to marginalized groups by talking about the broader issues of online harassment and privacy invasion. Marginalized groups, who often face heightened risks in online spaces, may be particularly more vulnerable to deepfake-related harm. From reading it, the study understands these concerns, emphasizing the need for fair protection.

Overall Societal Contributions

This article makes significant contributions to society by providing insights into the challenges of deepfake technology in the metaverse. It offers a practical management framework to address deepfake victimization, helping people learn online safety. Additionally, the study contributes to the research of technology, cybersecurity, and social sciences, and gives a multidisciplinary approach to potential threats.

In conclusion, "Victimization by Deepfake in the Metaverse: Building a Practical Management Framework" offers great insights into the metaverse's constant evolving ground and its impact on individuals and society. It combines different research methods, aligns with social science principles, and addresses important concerns, making it a valuable addition to the International Journal of Cybersecurity Intelligence and Cybercrime.

Article Review - "A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency"

Relating to Social Science Principles:

This article, "A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency," connects with several social science principles. It talks about the significance of comprehending societal, legal, and economic problems, particularly cryptocurrency. The study shows that the rise of cryptocurrencies like Bitcoin requires some research beyond just technical aspects, diving into the legal and regulatory frameworks that cross with society.

Research Questions and Hypotheses:

The research questions in the article revolve around understanding the common methods of money laundering via cryptocurrencies in Indonesia. It also talks about Indonesian laws and regulations that apply to such activities. While the article does not explicitly state a hypothesis, it implicitly explores whether existing legal and regulatory frameworks are effective in stopping/preventing money laundering through cryptocurrencies.

Research Methods:

The article employs a mixed-methods approach, combining legal analysis, regulatory examination, and a review of specific cases. It assesses existing legislation, such as Law No. 7 of 2011 and Law No. 23 of 1999, to understand their implications on cryptocurrency transactions.

Types of Data and Analysis:

Data in the article is primarily legal and regulatory texts. The analysis involves a comprehensive examination of Indonesian laws and regulations as it pertains to cryptocurrency

and money laundering. Specific cases of money laundering involving cryptocurrencies are cited to showcase the practical implications of the legal framework.

Relating to Concepts from Class:

The article relates to class by talking about the combination of technology, law, and society. We have talked about privacy laws for example. It also shows the need for a more in depth legal framework to govern cryptocurrency transactions,and the importance of interdisciplinary approaches in social sciences like the previous article. Additionally, the study shows how cryptocurrency regulations impact financial transactions and taxation, aligning with class discussions on how technology is rapidly advancing and how some laws can be out of date.

Challenges Concerning Marginalized Groups:

While the article does not directly discuss marginalized groups, it can indirectly address concerns related to financial inclusion and taxation. The regulations surrounding cryptocurrency can impact individuals across many socioeconomic classes, with potential inequality in access and taxation burden.

Overall Societal Contributions:

This study contributes to society by shedding light on the evolving area of money laundering in the context of cryptocurrency in Indonesia. It explains the importance of legal and regulatory frameworks in addressing financial crimes in the digital world. Furthermore, it offers insights into the implications of cryptocurrency transactions on taxation and financial transparency within the country.

In conclusion, "A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency" is a valuable contribution to understanding how emerging currencies like cryptocurrency can be involved with legal and regulatory frameworks. It highlights the importance of implementing these frameworks to address new challenges in financial crimes and provides insight for policymakers and legal experts in Indonesia and hopefully other countries as well.

References

Asfour, M. & Murillo, J. C. (2023). Harnessing Large Language Models to Simulate Realistic Human Responses to Social Engineering Attacks: A Case Study. International Journal of Cybersecurity Intelligence & Cybercrime: 6(2), 21-49. Available at: https://vc.bridgew.edu/ijcic/vol6/iss2/3

Manthovani, R. (2023). A Comparative Analysis of Money Laundering Crimes in Indonesia through Cryptocurrency. International Journal of Cyber Criminology, 17(1), 196–210. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/168/63