Your Name

Instructor Name

Course Number

Date

Cybersecurity and data privacy

**Introduction**

Cybercrime has become a major issue nowadays and this is done by computer specialists. The problem with the invention of technology and internet is that it risks the privacy of individuals. There is a need for cybersecurity and data privacy to ensure data protection of individuals. This paper will be discussing cybersecurity threats caused by computer specialists, big organizations, and political powers using social media platforms. However, there is a need to introduce strict ethical considerations with the help of artificial intelligence, which has to be followed by all social media and internet users.

**Summary**

*Fake news: A data-driven analysis of the role of influencers in the spread of misinformation and disinformation on selected social media platforms (Data manipulation and ethics)*

Article by Apampa, states that social media nowadays has become a source of communication and technologies like computer systems, and mobile phones have eased to use these social media platforms (1). Social media has many users, and it is hard to identify these users whether they are using social media for their own or they are using these media platforms to manipulate data, maybe for socio-economic gains or political gains. Social media platforms such as facebook, twitter, Instagram, and other media platforms have become a source for proliferation of fake news and information. In these recent years, fake news has taken ground, and it has become difficult to identify differences between fake and authentic news. While these fake news are designed to mislead, deceive the targeted groups, and individuals. This article includes a discussion about fake news on social media platforms, which misleads and misinforms all users, and other people as well. Through these social media platforms, data is manipulated, while ethical values for data and social media utilization are manipulated. Some rules and regulations are being set to ensure security and to avoid any data manipulation.

Unfortunately, computer experts, politicians, and other groups have manipulated data using social media. Data is manipulated for certain selfish gains, which are mostly political, social, and economic gains, and people are misguided by changing their perceptions and opinions. The proliferation of fake news is not a new concept; it is an old phenomenon. This fake news is a threat to freedom of expression of people, to democracy, and the greatest threat to journalism. Certain popular and significant have contributed to misleading people, and they have been involved in the manipulation of data by proliferating fake news, which has changed the opinions of people. Undoubtedly, challenging ethical consideration and proliferating fake news threatens democracy, electoral systems, decisions, government services, and economy.

Furthermore, the greatest threat is security of people and data, which is challenging the ethics of social media. These trends and increasing fake news threats have to be catered on time because they are challenging the democracy of nations, and importantly, it is changing opinions of people and users of social media platforms. These shifts in opinions are based on irrational thinking and disinformation, which may threat existing systems, which are for the welfare of people and may risk their security by welcoming selfish gains of popular personalities, especially politicians. Cybersecurity may be a source to control these threats, secure privacy, and minimize higher risks of disinformation proliferated among people using social media platforms. Cyber-attacks are one of the reasons involved in proliferation of fake news on social media platforms, computer experts, and hackers attack systems to control the data for their selfish gains. Cyber-attacks threat data privacy, there are chances that these originate from third parties who pay for manipulating data and damage first parties (Vitunskaite et al. 314).

*Better, nicer, clearer, and fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning*

This article by Greene and colleagues examines ethical concerns of artificial intelligence to develop ethical standards according to organizational backgrounds (2122). Ethical concerns and considerations vary from organization to organization, while ethical statements for them may lead to secure their data from manipulation by the third party's gains. Artificial intelligence can be understood from the designs of ethics, which are developed for ethical backgrounds. People are aware of ethical considerations, but they still violate while these can be controlled. Despite difficulties in finding sources, which hack systems and manipulate data of big organizations, there are sources such as artificial intelligence, which can be used to identify sources violating ethical considerations.

Setting high profile may help to construct and impose a collective ethical framework with the help of powerful instruments. However, these ethical frameworks only set and share a moral background regarding technological ethics. Besides, these help to develop a vision of artificial intelligence, which may be addressed using specific technical and design expertise. Unfortunately, taking these for granted and poor ethical considerations may result in harmful outcomes. The existing problem is that ethical scholars are being ignored only to avoid accountability in democracy, dominating processes of politics, large corporations, and these are equally responsible. While warning for ethical scholars is that they are unable to implement appropriate methodologies to avoid problems of people and devote social justice; rather, they are criticized for this, and ethical scholars are not recognized.

Developing ethical considerations and concerns means that Artificial Intelligence is developing different perspectives of people, and creates an understanding of people about systems, and functioning of Artificial Intelligence. While there are some systems, tools, and some groups of people are being developed to answer emerging threats and risks of cybersecurity by different communities, including scientific community and software groups. Ethical designs are similar to the concepts of Values Sensitive Design, and Principle for Accountable Algorithms, while algorithms are the creation of people. Humans are indeed responsible for the decision-making by these algorithms, and blaming these algorithms is not a logical answer. Therefore, humans must understand these systems properly and they have to develop a clear understanding of processes of machine learning. Lack of understanding of human-created systems may lead to bad consequences threatening data security systems of everyone, including big corporations, and political groups. These emerging threats lead humans to develop alternative systems in technology to avoid and minimize data threats, including security and privacy.

Unfortunately, there is a huge influence of big organizations and powers, which criticizes these ethical Artificial Intelligence concerns and considerations limiting in terms of technology and expert-views about the appropriate contribution of artificial intelligence. New products and services will be introduced by manufacturers to ensure security of data, but it is difficult because of competing interests of groups (Vitunskaite et al. 316). Self-interests and gains, which include organizational approaches towards security of data, are responsible for an increase in levels of risks to stakeholders and manufacturers.

*Smart cities and cybersecurity: Are we there yet? A comparative study on the role of standards, third party risk management, and security ownership*

This article journal by Vitunskaite and colleagues starts with the discussion of smart cities, which are revolutionizing lifestyles of people (313). The aims of these revolutions include a reduction in costs, economic efficiencies, and reduction in environmental outputs. Smart cities themselves are in their initial stages, which completely relies on the innovations and technologies, opens sources to identify professional attackers and criminals, which may cause harm to big organizations. Smart cities are adopting new trends to secure their data and other data, ensuring avoidance of any further threat related to cybersecurity and data privacy. However, smart cities are still facing issues of technology, standards of security, regulations of security, and data protection.

There are emerging threats from third parties, who are involved in the development, and manufacturing of new devices and software, while these devices and software are directly linked to consumers in ecosystem of smart cities. These are hopeless because of a lack of control over security risks, they have to take responsibility for their systems on priority, and they have to open up about new breaches taking place in these cities. Smart cities can present an appropriate framework, which ensures cybersecurity in overall layers existing in smart cities. Third parties are involved in data breaches and manipulation, while primary organizations are held responsible for this and they have to pay.

Social media users intend to follow what they have been observing, and they start trusting the information, which is promoted to their screens. Users agree to give access to their data, consciously or unconsciously but they do for sure, while this shows that they trust devices and software, which they are using. In smart cities, they believe that trusting data is important to operate smart cities but the problem is that cyber attackers are potential and they can attack their operations. Smart cities have to ensure data security of people and there have to be safer ways of data sharing within the ecosystems of these smart cites. While leadership may help to handle these security threats without looking for their political gains, and there is a need for governance to introduce new security systems to improve cybersecurity with ethical concerns, and accountability of third parties and data attackers.

**Analysis**

I believe that cybersecurity threats have increased, especially fake new revolving around social media, which manipulates authentic data, and another problem that has increased is cybersecurity. Cybersecurity is at risk because of influential people and big organizations, which are looking for their gains and benefits for their future. Disinformation has changed perceptions and opinions of people, which has made an impact on decision making of people towards elections, democracy, and governances by their states. Data attackers are making a profit by harming data of people and they are putting privacy of people at risk. I believe that manipulation of data is referred as cybercrime and to control it there has to be a platform such as a smart city. This ensures to provide security and saves the data from manipulation from the data hackers.

Including cyber scholars, who ensure cybersecurity in their consideration, but they are ignored because of the influence by political powers and organizations. Their suggestions regarding ethical considerations and frameworks have to be recognized to ensure cybersecurity. Despite being influenced by political and big organizations, ethical scholars and smart cities have to develop new perceptions and developments, which will encourage data ethics and cybersecurity. If this is not done one time, then people will be losing their identity, and there will be no concepts of privacy, their will decisions will be based on the information, which these big powers want them to know.

**Conclusion**

There are still chances to increase influence of ethical scholars to ensure healthy use of social media and innovative technology without harming others and without changing decision powers of individuals. Awareness about identification of information sources has to be made sure because this is the only reason, which changes decisions and perceptions of people. Accountability by government to control cyber attackers and accountability of government segments who influence decision-making of people for their gains have to be restricted.

Works Cited

Apampa, Olatunji. *FAKE NEWS: A DATA-DRIVEN ANALYSIS OF THE ROLE OF INFLUENCERS IN THE SPREAD OF MISINFORMATION AND DISINFORMATION ON SELECTED SOCIAL MEDIA PLATFORMS*. 2019. *ResearchGate*, doi:10.13140/RG.2.2.14257.84320.

Greene, Daniel, et al. *Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning*. 2019. *scholarspace.manoa.hawaii.edu*, doi:10.24251/HICSS.2019.258.

Vitunskaite, Morta, et al. “Smart Cities and Cyber Security: Are We There yet?A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership.” *Computers & security*, vol. 83, June 2019, pp. 313–31. *ScienceDirect*, doi:10.1016/j.cose.2019.02.009.