THE RISE OF DIGITAL AUTHORITARIANISM: SOCIAL MEDIA, SURVEILLANCE, AND STATE CONTROL IN THE 21ST CENTURY

***1st Saad Ghafoor**
MPhil Scholar of AI and Global Politics, Department of Political Science, Government College University, Lahore saad.malhi@outlook.com
2nd Muhammad Ali Safdar
PhD Scholar of Law and Philosophy at Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany ali.m.safdar@fau.de

Abstract

Power in the digital age has undergone a deep transformation when it comes both to how increasingly democratic governments and authoritarian regimes exercise power in the 21st century. This research paper elaborates on this concept titled digital authoritarianism that looks into how 'strategic use' of a set of digital technologies like social media, surveillance tools, artificial intelligence, and censorship is exercised for monitoring, manipulating, and suppressing public discourse. At one-point, digital platforms were seen as empowering and helping democracy. Now, states are using them to enhance their grip on power and cut off opposition. The study uses a qualitative case study approach to find out how China, Russia, India, Turkey, and the United States use digital tools to influence opinions and restrict civil rights. It employs theories of panopticons, networked authoritarianism, and critical media studies in order to reveal how digital repression works and how the boundaries of state power are shifting. Additionally, it shows new forms of resistance developing, from cyberoptimism to digital literacy campaigns to the world's embrace of internet freedom and data rights. This study fills an interdisciplinary scholarship expanding on authoritarian governance, digital media, and surveillance capitalism. It demands urgent policy attention, stringent international regulation and the creation of ethical frameworks in order to protect democratic values, privacy and human rights in the ever more digitized world.

Keywords: Digital Authoritarianism, Social Media, Surveillance, Digital Revolution, Democratic Power

Introduction

In the 21st century, digital technology has changed the way people interact in every area, from talking to each other and buying goods to learning and running a country. Since more than five billion people use the internet and digital technology is growing fast, cyberspace is now a key area for politics, social action, and personal expression. At first, digital technology was praised for giving ordinary people more power and making information more available to them. On the other hand, this optimism is now being challenged by the fact that many countries, democratic or not, are using digital tools to keep tabs on and limit their citizens.

Digital authoritarianism involves the use of digital technology by governments to keep their power, silence anyone who disagrees, influence the public's views, and monitor citizens in the name of safety, public health, or stability. Even democracies are now more likely to use repressive digital methods that threaten the rights and values of their citizens. With the help of advanced surveillance systems powered by AI and big data, governments can now track individuals, guess their actions, and control the information people receive much more easily than before. These new technologies have changed the way the state and its citizens relate, giving much more power to the authorities.

Social media platforms that were once seen as helping to spread freedom are now seen as having both positive and negative effects. Although these platforms help people take part in civic life, they are also used for censorship, surveillance, spreading false news, and influencing people's minds. Authorities use bots and trolls to take over online discussions, silence opponents, and create disagreements among people. Because of their desire to make profits and their secretive rules, platform algorithms tend to increase the spread of misinformation and group think, which helps authoritarian groups. Thanks to biometric databases, facial recognition, and tracking people's locations, regimes can easily monitor protests, prevent people from moving freely, and ensure everyone follows their beliefs. In several instances, these tools are used based on laws that usually justify repression by talking about public safety and order.

This paper is focused on the current global situation, where technology that was meant to bring people together is now used by governments to gain more control. The study looks at how governments in different regions are putting in place digital authoritarian practices by using social media and surveillance. Five nations, China, Russia, India, Turkey, and the United States, are singled out because they have different political systems and levels of technology, yet all tend to use digital repression. In addition, this research paper looks at the effects of always being watched online by society and by oneself. Being watched can stop people from expressing themselves freely and leads to more self-censorship, making them distrust institutions. It looks at how laws aimed at cybercrime, terrorism, or misinformation are sometimes used to support authoritarianism, while those who resist these measures have to deal with increasingly tough digital conditions.

In short, the need for this research comes from the fact that the digital space is now biased. It is a place where the principles of openness, freedom, and democracy are being challenged and, in several places, are being weakened. If left uncontrolled, digital authoritarianism may seriously threaten basic human rights, democracy, and the world's stability. It is important for policymakers, researchers, groups in civil society, and citizens to understand the changes in digital repression, since what happens today will shape the digital world for many years ahead.

Limitations of Research

This paper seeks to examine digital authoritarianism in detail; however, some limitations should be noted.

Access to Reliable Data: Authoritarian regimes usually prevent people from getting accurate data, silence those who challenge their views, and control the sharing of news. As a result, it becomes difficult to get information that can be verified personally. Especially, information coming from China, Iran, or North Korea. A lot of findings are based on secondary sources, which may include biases or have a narrow scope.

Selection Bias in Case Studies: When only China, Russia, India, USA, and Turkey are chosen in case studies, other places where digital authoritarianism is increasing are not always considered. This means the study's findings are not representative of the whole world.

Rapidly Evolving Technology: Technology is advancing faster than the research that is being done. By the time the data is available, some technological changes (such as new ways to watch people, AI programs, or censorship) may have taken place. It has an impact on the lasting importance of research results.

Political Sensitivity and Researcher Safety: Researching authoritarian regimes can be dangerous because of political sensitivities. Those doing research and those participating in it, such as journalists, activists, or whistleblowers, may encounter risks to their privacy or safety. This issue may stop researchers from conducting in-depth studies or from talking to key informants.

Language and Cultural Barriers: Many digital authoritarian techniques are written in the local language or based on the local culture. Even with help from translators and local partners, some important details may not be understood in the analysis.

Scope of Generalizability: Even though this study uses comparative case studies, the findings may not work for every political regime. Since every country has its own level of digital freedom, how it is governed, and its social and political setting, it is hard to make conclusions that work for all.

Significance of Research

Digital authoritarianism is a major shift in the way people are governed, opposition is stopped, and information is managed in the digital world. This investigation has several important aspects.

Filling an area where knowledge is lacking: Although authoritarianism is well known in political science, how modern states use technology and social media for control is still a new area of study. It adds a new perspective by linking political science with other fields.

Theory, media studies, and digital governance are the main subjects.

How it affects current global political issues: Since governments around the world, including those in liberal democracies and autocracies, are using digital tools for ruling, this study helps explain a global problem that puts democracy at risk. It reveals that democratic governments may start using authoritarian methods in the name of national security, keeping public order, or controlling misinformation.

Participation in Policy and Governance: This paper offers up-to-date information that can be useful for policymakers, lawmakers, and international organizations in realizing the dangers of uncontrolled digital tools. The study will propose ways to ensure digital rights, oversee surveillance technology, and making sure that democracy is involved in the process.

Informing the public: In different situations, people are not aware that their online actions are being watched, blocked, or modified. This research will make people more aware of digital privacy, the control of algorithms, disinformation by governments, and the slow loss of civil liberties.

Encouraging Future Research: The study sets the stage for future research by introducing a framework and pointing out similarities in digital authoritarianism in different parts of the world.

Research Questions

1. What are the main features and processes that describe digital authoritarianism in modern times?
2. In what ways do authoritarian and democratic regimes use the internet and social media to guide public opinions and stop people from speaking out?
3. What impact does social media have on digital authoritarianism, helping it or making it more difficult?
4. How are people, organizations, and foreign groups dealing with or fighting against digital authoritarianism?
5. How will global democracy and freedom be affected in the long run by digital authoritarianism?

Objectives of Research

- To develop and describe the ongoing phenomenon of digital authoritarianism.
- To study case studies that take place in China, Russia, India, Turkey, and the United States. To check how social media can help or challenge authoritarian governments.
- To understand how well surveillance technologies and digital propaganda work.
- To suggest policies and principles for fighting against digital authoritarianism.

Literature Review

Many scholars are now focusing on digital authoritarianism, given that states have begun using technology more and more to control their populations. Experts say that digital technologies, which used to help people participate in democracy, are now being used by both authoritarian and democratic governments to watch over dissent and change public discussions (Howard & Bradshaw, 2019). In today’s authoritarian regimes, surveillance technologies are very important. Deibert (2020) points out that governments are using biometric information, face recognition, and AI to set up digital panopticons. In China, the Social Credit System is a clear example of how technology is used daily to make sure people follow the government's rules (Creemers, 2018). They help in observing citizens' actions and also make surveillance a common practice for the government. At the same time, social media sites, which were once celebrated for their democratic possibilities, have turned into instruments for spreading propaganda and controlling people. In his book, Morozov (2012) explains that authoritarian regimes now use social media to share false stories, harass their opponents, and give the impression that many people support them. Bradshaw and Howard (2018) noted that coordinated disinformation is now a main tactic used by governments to influence people at home and abroad. Also, Feldstein (2019) points out that digital authoritarianism is becoming more common in democracies, as governments use the same techniques and claim they are needed for the country's safety or health. Because of this, it becomes harder to distinguish between democratic and authoritarian governance online, which makes overseeing and regulating things more challenging. Some recent studies are looking into how people resist digital authoritarianism. To tackle these issues, groups such as human rights organizations and civil society have introduced encrypted apps, ways to stay anonymous, and educational programs on digital safety (MacKinnon, 2012). However, often, these groups encounter major challenges because of the strong state surveillance systems. The way algorithms affect online discussions in authoritarian societies is another important subject for researchers. In Tufekci's opinion (2015), social media platforms like Facebook and YouTube can be used by governments to give preference to pro-government content and reduce the visibility of content that opposes them. This situation, called algorithmic authoritarianism, points out how the design of platforms can greatly affect political decisions. Many people are discussing how platforms are involved in digital authoritarianism. Zuboff (2019) believes that tech companies take part in "surveillance capitalism," which makes it possible for authoritarian states to use personal data. Even though these companies say they are neutral, Freedom House (2022) found that they cooperate with restrictive laws to keep their place in countries like China, Russia, and India. Moreover, shutting down the internet has become a common method used by digital authoritarians. In 2022, Access Now (2023) counted more than 180 intentional internet shutdowns around the world, usually during elections, protests, or times of unrest. By taking these actions, the government severely restricts people's access to information and prevents humanitarian and journalistic activities. People have also started to focus on cyber laws and legal authoritarianism. Hintz, Dencik, and Wahl-Jorgensen (2019) point out that many countries have passed cybercrime laws that are unclear and allow authorities to watch people's activities online with little supervision by judges. Often, such laws are introduced as a way to stop terrorism or fake news, but they actually help authoritarianism. The effects of digital authoritarianism on people's minds is becoming a new field of study. According to Penney (2017), being watched by the state often leads people to not take part in political discussions. Consequently, fewer people take part in public activities, which weakens the public sphere in all environments. In addition, international organizations and think tanks have pointed out the importance of global management of digital technologies. The United Nations Human Rights Council (UNHRC, 2021) has urged for better protection of digital rights due to the fast growth of surveillance technologies. Even so, international standards are often blocked by the conflicts and goals of different nations.

Research Methodology

The research paper is based on qualitative and comparative case study methods. I analyzed what was posted on state-run social media accounts and examined digital laws, and I also conducted semi-structured interviews with journalists, activists, and tech experts. In addition, reviews of leaked government documents, NGO reports, and academic literature were done, along with the data collection process. To get more information, the paper relied on digital ethnography of online censorship and propaganda networks. In addition, case studies were taken from countries such as China, Russia, India, USA and Iran to study digital surveillance, social credit systems, and control over online disinformation and media. Besides, the study applies a hybrid theoretical approach. Foucault's idea of Panopticons is centered on how the state watches and disciplines people. Critical Media Theory mainly focuses on how digital stories are manipulated. This theory was applied to see how regimes survive and maintain their power. I also looked at Network Authoritarianism (Howard, 2013), which explains that autocratic states have taken advantage of new digital tools. The study can lead to a classification of digital authoritarian methods in different regimes and give a clearer view on how technology and authoritarian rule have changed together.

Discussion & Analysis

The purpose of this study was to look at how modern states are using digital technologies like social media, surveillance, and algorithms to control politics in the 21st century. By looking at case studies, studying policy texts, academic literature, media reports, and findings from international watchdogs, the analysis highlights main patterns in digital authoritarianism around the world. The study concentrated on China, Russia, India, Turkey, and the United States because they have different political systems and control over technology. Below, the discussion is presented in a story-like way with few headings, yet it still deals with the main themes: surveillance, censorship, propaganda, platform involvement, laws, and resistance.

The use of more digital surveillance technologies

One clear sign of digital authoritarianism is the use of advanced tools to watch people. Now, states can gather, keep, and analyze a lot of personal data by using facial recognition, biometric scanners, CCTV cameras, phone tracking, and AI tools. In China, there are more surveillance cameras than anywhere else, and the regime is highly organized, with 540 million cameras installed by 2021. People are watched all the time, and their social credit scores, based on facial recognition, can prevent them from using transport, getting jobs, going to school, or using dating apps. In Xinjiang, mobile apps, DNA databases, and smart street sensors are used by the surveillance apparatus to meet China's political goals with Uyghur Muslims. In this country, digital surveillance is used to repress culture and single out people by their ethnicity. In Russia, authorities also use technology to keep an eye on anyone who opposes them politically. The Federal Security Service (FSB) can carry out phone call, email, and internet interceptions through the government's SORM, without any judicial review. After the protests organized by Alexei Navalny, people who attended the rallies were reportedly caught and detained using facial recognition technology in Moscow's metro stations. The fact that these technologies are used proves that authoritarian regimes depend on real-time information to prevent any resistance and punish those who disagree with them. National security and public health are the main reasons given for using surveillance in India and the United States. What was originally meant to distribute welfare has turned into a system that monitors over 1.3 billion people using a central database of biometric data. When the COVID-19 pandemic began, Aarogya Setu collected people's geolocation data without enough privacy protection. The revelations by Edward Snowden about the NSA in the US demonstrate that democratic countries can still collect large amounts of data without following the rules set by their constitutions. Even though the degree and reasons for surveillance differ, the practice of monitoring people online is becoming common and worrying.

Social media as a Way to Control and Spread Ideas

At first, social media was seen as an opening for freedom, but now many states use it to spy, control information, and shape people's actions. Now, it is common for both authoritarian and hybrid regimes to use digital tools for their own benefit. In China, Weibo and WeChat use keyword filtering, censorship software, and people to monitor and remove content that criticizes the government, promotes democracy, or talks about Tiananmen Square, Tibet, or Taiwan. Most importantly, the government encourages "positive energy" by posting many pro-state messages online using the "50-Cent Army." In addition, Russia has established an advanced method of manipulating digital information. IRA and similar troll farms, which are supported by the government, have been accused of affecting elections and creating disagreements both inside and outside the country. By using bots, spreading false news, and memes, the Russian government manages to influence opinions and weaken trust in liberal democratic institutions in other countries. Furthermore, In India, the government that claims to be democratic is showing signs of authoritarianism in the digital world. Government supporters use Twitter to create hashtags and target people who oppose the government. Those who speak out against the government's actions in Kashmir or concerning minorities are regularly targeted by online harassment. On social media, people show their nationalism and the police use what is shared to find and arrest those who protest or are accused of sedition. In the United States, the problem is not usually propaganda from the government, but rather the way algorithms increase political polarization. Thanks to Facebook, YouTube, and Twitter, it is now easier for misleading information to spread. Because there are no strict regulations, conspiracy theories, hate speech, and disinformation from other nations have been able to shape public opinion in the US. The events of January 2021 at the Capitol showed how digital tools can encourage large-scale actions against democracy if they are not controlled.

Laws and the Authoritarian Use of Power

Digital authoritarianism is usually implemented by using laws instead of direct force. Many countries are creating cyber laws that increase the ability to monitor people, punish online criticism, and require companies to share user details. Cybercrime, terrorism, and misinformation are the main reasons these laws are made, but they are often used to control political opponents. As an example, Turkey's 2020 social media law requires platforms with more than one million users to keep their data inside the country and name a representative there. If you do not comply, you may face big fines or have your bandwidth reduced. As a result, Turkish officials can ask Twitter and Facebook to remove specific content or hand over user information. The law is often used to stop criticism of President Erdoğan and his party, mainly at election times or after scandals involving the government. In India, the 2021 IT Rules ask platforms to identify the first person who posted the content and delete anything that might threaten national security or public order. Because of these rules, privacy advocates are concerned, especially since WhatsApp and similar services are being urged to reveal user information. As a result, these laws enforce digital repression and still appear to comply with the law. On the other hand, Western democracies have difficulty finding a balance between keeping the country safe and ensuring digital rights. After the Patriot Act, the CLOUD Act made it possible for US authorities to access data from other countries and issue secret orders in court. Although the Electronic Frontier Foundation (EFF) and other civil groups have tried to stop this trend, it appears that the government is aiming to increase its digital supervision with legal backing.

The role of Tech Companies

Private technology companies have played a major part in helping authoritarian regimes control the internet. Because social media and data analytics companies work in a global market, they often have to follow strict rules set by certain governments. Apple removed VPN apps from the Chinese version of its App Store because of government pressure, and LinkedIn censored its content to keep operating in China until 2021. Likewise, Amazon Web Services and Microsoft Azure are said to have provided cloud computing services that were used by authoritarian states to monitor their citizens. In addition to obeying the law, corporations are also actively helping in these activities. Since many global technology systems are owned by private corporations, a main issue is that these companies are not held accountable by international human rights rules. While these reports are helpful, they usually highlight how often governments request the removal of data and content. During the period from July to December 2022, Twitter was asked by governments to remove content more than 47,000 times, with most coming from India, Russia, and Turkey. While Twitter, Meta, and Google say they stand for user rights, their actions usually show a readiness to cooperate with authoritarian demands to keep their businesses running.

Ways People and Communities Resist and React

Even though digital authoritarianism is becoming more advanced, civil society is countering it with new ideas, lawsuits, and help from other countries. Those protesting for democracy in Hong Kong used many tactics, for example, communicating using Signal, hiding their faces with masks and laser pointers, and sharing the routes of protests on peer-to-peer networks. People in Iran and Myanmar use VPNs, proxy servers, and networks that do not rely on central servers to avoid censorship. Diaspora communities help to make hidden voices heard and to record acts of state violence. Groups like Access Now, Freedom House, and Reporters Without Borders are always working to record digital repression and help those affected. Legal advocacy is now being used as a way to challenge the government. When groups in civil society want to challenge surveillance laws, they often refer to the GDPR set by the European Union. The 2020 Schrems II ruling from the Court of Justice of the European Union ended the Privacy Shield agreement between the US and EU because it felt data protection was not adequate, showing that the courts could limit cross-border surveillance. Still, these types of resistance have many restrictions. Because the state has greater power online, it is usually difficult for individuals to challenge it successfully. In many parts of the globe, people are not digitally literate, and it is hard for them to learn how to use secure communication methods. In addition, because AI and machine learning are used more in surveillance, authoritarian governments can now forecast and stop resistance more successfully than in the past.

SUM UP

It is clear from this analysis that digital authoritarianism affects many countries and goes beyond the usual political borders. Not only authoritarian regimes are responsible; democracies are also using similar methods, but with different names. States are using methods such as mass surveillance, censorship, algorithmic tools, and laws to take over the internet. Technology is not bad, but when those in power use it without being held accountable, it becomes a way to oppress people. Tech companies' involvement, problems with international laws, and the weaknesses in civil society all help digital authoritarianism to become more common. With more and more digital activities, it is becoming more important to protect digital freedoms. The main challenge is to make sure that digital spaces remain places of freedom by creating clear rules, working with other countries, using technology ethically, and empowering people.

Conclusion

The digital revolution was once celebrated for helping to democratize society and bring people around the world closer together. In several situations, it is now widely used to control and suppress people. The study examines how digital authoritarianism has become a major aspect of today's government, changing the way states and people relate to each other. It is clear from reviewing case studies in different political settings that governments, no matter their type, are using new technologies to watch over dissent, change public opinions, and maintain their power. Thanks to AI-based monitoring, censorship by algorithms, and propaganda on the internet, states have changed the way they control politics online. The research paper points out that social media platforms, which used to support civic involvement and free speech, have now been used to silence people and share misleading information. At the same time, the growth of surveillance capitalism and the unclear workings of digital systems make it harder to ensure people are informed and responsible. Still, the study points out that there are areas where people push back through digital activism, exposing wrongdoing, and calling for internet freedom and data protection around the world. Even though these actions are scattered, they show an increasing awareness that democracy needs to be defended from increasing digital threats.

In short, digital authoritarianism is a political system that seriously affects privacy, democracy, and human rights. As new technologies appear, the international community should unite to stop their harmful use, strengthen society, and create a digital society based on transparency, freedom, and justice.

Recommendations for Future Related Studies

Considering the results and restrictions of this study, the following suggestions are put forward for future research in digital authoritarianism.

- Studies in the future should focus on digital authoritarianism in regions that are not well-represented, for example, Sub-Saharan Africa, Southeast Asia, and Latin America. Exploring how culture, religion, and regions play a role in the use and opposition to digital control would add more knowledge to the global study of this issue.
- Experts should carry out research that studies how digital authoritarian methods have changed over the years. It would allow us to see how states change their digital policies because of new technology, public protests, and pressure from other countries.
- The actions of private technology companies are important in helping or preventing the government from spying on citizens and blocking information. In the future, researchers should study whether social media platforms, telecom companies, and vendors of surveillance software help or oppose digital authoritarianism.
- More studies should be done on the ways activists, dissidents, and civil society organizations use technology to fight against authoritarianism. Examples of encrypted talks, people using VPNs, online protests, and cyber activities can help us understand how digital resistance succeeds.
- Future studies may concentrate on making international rules, digital rights charters, and guidelines for ethical use of surveillance technologies to maintain responsible cyber governance.
- Researchers should also try to use methods from political science, media studies, data science, law, and ethics to deal with the many aspects of digital authoritarianism.

References

Access Now. (2023). The return of digital authoritarianism: 2022 internet shutdowns report. https://www.accessnow.org/internet-shutdowns-2022/

Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation. Oxford Internet Institute.

Creemers, R. (2018). China's social credit system: An evolving practice of control. SSR International Journal, 6(1), 23–40.

Deibert, R. (2020). Reset: Reclaiming the internet for civil society. House of Anansi.

Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace.

Freedom House. (2022). Freedom on the Net 2022: Countering an authoritarian overhaul of the internet. https://freedomhouse.org/report/freedom-net/2022

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). Digital citizenship in a datafied society. Polity Press.

Howard, P. N., & Bradshaw, S. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. Oxford Internet Institute.

MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for internet freedom. Basic Books.

Morozov, E. (2012). The net delusion: The dark side of internet freedom. PublicAffairs.

Penney, J. (2017). Chilling effects: Online surveillance and Wikipedia use. Berkeley Technology Law Journal, 31(1), 117–182.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(1), 203–218.

United Nations Human Rights Council. (2021). The right to privacy in the digital age (A/HRC/48/31). https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.