مجلۀ علمی – تحقیقی تاج
Taj Academic and Research Journal

Date received :4/8/2024
Date accepted:14/10/2024
Print ISSN: 2664-9144

Digital Privacy Violation with a Focus on the Consequences and Supporting Mechanisms in the National and International Documents

Safa Barakzaei[1], Maryam Mohammadi[2]

Abstract

The emergence of the internet has changed the way people communicate and has sparked a new social revolution in which privacy is a prominent debate. The information age, with the expansion of virtual spaces, has jeopardized privacy and even led to privacy violations, resulting in diverse consequences, and to protect digital privacy, national and international documents have also been developed. The research question is: Which authorities have violated privacy in the digital world, and what are the consequences? Which international documents recognize the protection of privacy in the digital world, and what is Afghanistan's position in this regard? Digital privacy is violated by the governments, technology companies, and individuals and has economic and psychological consequences. Also, the right to privacy is recognized in international documents such as the Universal Declaration of Human Rights, with Afghanistan having a weak position. The main goal of the study is to examine digital privacy violations with a focus on the consequences and supporting mechanisms in the international and national documents. The type of research is mixed-method (qualitative and quantitative). Initially, it delves into discussions on digital privacy violations based on literature from books, articles, and websites. Subsequently, it concludes with a survey analyzed using SPSS software.

Keywords: Privacy, Digital World, National and International Documents, Violation, Consequences .

1 . Law and Political Science undergraduate of Herat University “safabarekzai22@gmail.com”
2 . Law and Political Science undergraduate of Herat University “maryam.moh104@gmail.com”

1. Introduction

The advent of the Internet has changed the way people communicate with each other, and a new social revolution is currently underway. Modern society evolved from agriculture to industry and now relies on digital technology, connecting identities, cultures, and relationships globally.

Privacy is inherently in such a way that it cannot be defined exclusively. This privacy may vary from society to society and from time to time. Among the various definitions of privacy, it can generally be said that privacy is the boundary of a person's life that is determined by laws or custom in such a way that the arbitrary interference of others in this boundary causes emotional and mental discomfort to people; in other words, it causes the injury and humiliation of their feelings by others. Privacy has been one of the most fundamental human rights, although society has not yet reached an acceptable level to protect people's privacy. This right has been recognized as an important principle in regional and international law, and a number of laws have been approved in this field .

In the digital age, privacy faces unprecedented risks due to advancements in information technology and virtual spaces. While innovations in communication technologies offer new ways to uphold fundamental rights and document violations, they also introduce significant challenges. Privacy breaches can occur through individuals, governments, or technology companies. The rapid evolution of science and technology has introduced new threats to privacy, making it a critical issue. Governments, companies, and individuals must each adopt specialized measures to safeguard privacy and address these emerging threats effectively.

The importance of communication and information technology in the modern and present world has been undeniable, and these technologies have brought valuable advances to society with the unprecedented growth of technology. While digital technologies and services create opportunities and challenges to strengthen, protect, and advance human rights and fundamental freedoms, digital technologies can be used for malicious purposes through a variety of malicious activities, including widespread surveillance and control. Since the right to privacy in the digital age must be a human right and must be protected, this right has always been suppressed and violated by certain individuals and organizations in this era. The speed and changes in the digital world require research on conflicts and disruptions related to the privacy of individuals, whether the right to privacy is protected or not. To clarify such issues, it is necessary to conduct research on how to protect individuals' privacy rights and how to prevent violations of their rights.

The innovative aspect of the mentioned research is that it has examined the violations of privacy in the digital world in Afghanistan and the role of governments, companies, and individuals to protect privacy. This investigation is done using a survey and according to the years 2023 and 2024 so that we can reveal the issue accurately and statistically .

1.1 Research Questions

1. What is digital privacy ?
2. What responsibilities do governments, companies, and individuals have in protecting privacy in the digital world?

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

3. Which international documents recognize the protection of privacy in the digital world, and what is Afghanistan's position in this regard?
4. Which authorities have violated privacy in the digital world, and what are the consequences?

1.2 Research Objectives

1. Examining the definition of digital privacy .
2. Examining the responsibilities of governments, individuals, and companies in protecting privacy in the digital world.
3. Examining privacy protection in the digital world in national and international documents.
4. Examining privacy violation and its consequences in the digital world.

2. Literature Review

In the modern world, with the growth and development of technology, the issue of privacy has become a key topic globally and especially in Afghanistan. Although much research has been conducted in this area, it seems that privacy violations have increased significantly, and these violations may occur from governments, companies, and even ordinary individuals. Given the extent and complexity of this issue, there is an increasing need for in-depth analysis and the development of effective solutions for privacy protection.

In 2016, Allessandor Zamboni and others published a study titled "Privacy in the Digital World: Beyond Compliance, Towards Trust." This study, after defining privacy, examines a survey conducted in 2016 across France, Italy, Germany, China, the USA, and the UK. The focus of the survey is on people's trust in the digital world and highlights that individuals in these countries are concerned about their privacy in the digital realm as new technologies increase their fears. The study concludes by discussing the future of privacy in the digital world and how we can prepare for new developments with the advancement and growth of new technologies.

In 2017, Lena Köhler, Sean Woodard, and Juliane Damen conducted a study titled "The Human Right of Privacy in the Digital Age," which addresses the challenges of the right to privacy in the international legal domain. The study first provides a general definition of privacy and presents an international legal framework. It highlights the role of technology and companies like Microsoft, which increasingly bear the responsibility of protecting digital media from misuse, surveillance, and the unjustifiable collection and storage of data. Finally, the study also discusses individual accountability regarding the right to privacy.

In 2019, Elham and Mahdi published an article titled "Examining User Privacy in Cyberspace to Propose Solutions for Its Protection." This article aimed to provide a systematic approach to analyzing the threats and risks in the realm of security and privacy in cyberspace and also reviewed the proposed solutions found in various sources and scientific articles.

3. Research Methodology

This research uses a mixed-methods approach (quantitative and qualitative) to conduct an in-depth analysis of issues related to privacy violations in the digital world, their consequences, and international and national documents. The first section of the study, titled "Theoretical Framework," provides a comprehensive introduction to the topic. This section includes theoretical discussions on the definition of privacy, its history, and crimes against privacy in the digital age. The sources used in this section include books, articles, websites, and reputable reports.

The second section of the research is dedicated to "Research Findings." In this part, data was collected through a survey and the distribution of a questionnaire among residents of Herat. Content analysis was performed using the SPSS program to obtain precise and scientific statistical results. This method allows us to conduct a more accurate analysis and interpretation of the issues related to the topic, considering field data.

4. Theoretical Framework

4.1 .Privacy

One of the most fundamental human rights is the right to privacy, upon which all other human rights rest and are deemed essential components. We can use this privilege to set boundaries with other people, preventing them from meddling in our personal affairs or privacy .

American professor Tom Gerety expressed privacy as “the control over or autonomy of the intimacies of personal identity.” American Edward Bloustein stated that intrusion into privacy has a close connection with personhood, individuality, and human dignity (Adrienn, 2016: 258). Privacy is seen as the possibility for an individual to retain some form of anonymity in his or her activities and to have the ability to isolate oneself in order to best protect his or her interests, so it is intimately linked to the notion of freedom (Zamboni et al., 2016: 10).

In our opinion, privacy is the area where a person wants to protect the realm of his personal material and spiritual life from the eyes of the public, and the general meaning of the right to privacy can be defined as follows: All natural and legal persons have the right to protection of their material borders (house, documents, and land) and spiritual borders (reputation, honor), whether online or offline, so that no one can interfere arbitrarily in their privacy without considering the laws of their country.

4.2 The History of the Relationship Between Human Rights and Privacy

Human rights are rights inherent to all individuals by virtue of their humanity, and each person possesses inherent dignity, an unalienable right not granted by any country or government.

The recognition of privacy as a human right finds deep roots in human history. Throughout different periods and societies, including traditional and primitive communities, rules existed to delineate the boundaries of individual privacy, such as restricting access to specific locations or prohibiting entry in certain areas. Legal scholars assert that personal privacy has a rich legal history, with Warren and Brandeis's pioneering research in the 1980s marking the first substantive and explicit discussion of individual privacy within legal frameworks. At the international level, most countries across Asia,

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

Europe, the Americas, Africa, and Australia have enacted laws to safeguard privacy. Consequently, privacy is not only recognized as an individual right but also as a social value (Fathi & Shahmoradi, 2017).

The essence of privacy is intertwined with the existence of the individual, and privacy gains significance and recognition in tandem with the importance of the individual. Without an individual, whether a natural or legal person, privacy becomes trivial and inconsequential, so it can be argued that the existential philosophy of the right to privacy traces back to the philosophical essence of personhood, linking the two closely and intricately.

4.3 Privacy in Digital Age

The Internet is a network consisting of millions of local, public, academic, commercial, and governmental networks that are interconnected by wireless and optical electronic technologies. Moreover, the Internet has a wide range of informative sources and services, such as web pages on the World Wide Web or e-mail (Arbani & Vahedi, 2019: 3). The role and importance of digital communication and information technology are undeniable in the 21st century, and we can boldly say that the gap between people's presence in the digital space and the real world is closing rapidly .

Due to the importance of privacy, there are many people who are concerned about their privacy, which someone else might breach. The purpose of digital rights is to promote the use of data privacy by respecting technologies. In addition, these technologies must respect intellectual property rights, prevent misinformation, and protect human rights (Hlophe, 2023). In September 2019, the United Nations General Assembly affirmed that all rights that people have offline must be protected online (Joyce, 2015).

These technologies and digital services, in addition to creating opportunities and challenges to strengthen, protect, and promote human rights, including privacy and fundamental freedoms, can also be used for malicious purposes and abused through a variety of malicious activities, including misinformation, surveillance, and extensive controls to limit the civil space and public discourse. For example, on the Internet, things and connected devices can collect data about daily habits, such as sleep patterns, physical activity, and consumer preferences (Zamboni et al, 2016).

4.4 Crimes against Privacy in the Digital Age

Crimes against privacy in the digital age involve acts committed to harm an individual's reputation or cause physical or mental harm using computers and/or networks such as the Internet or mobile networks. Cybercrime encompasses criminal activities targeting computers, computer networks, or network devices. Cybercriminals are often motivated by financial gain, but political and personal motivations are also common .

Online harassment, occurring on platforms like social media, forums, email, and instant messaging, involves actions such as creating fake profiles, spreading rumors, sending unpleasant messages, and using hate speech (Khatri, 2023). It refers to the intentional use of information and communication technology to harm others repeatedly. Forms of online harassment include trolling, cyberstalking, revenge porn, and cyberbullying (Gauri, 2023).

"Hacking" refers to actions aimed at undermining digital devices, including computers and networks. Hackers have various motivations, including political, personal, and financial reasons. The term originated at MIT in the mid-1900s, initially referring to tampering with train sets (Biggest Hacks, 2023).

"Internet fraud" involves fraudulent schemes presented to potential victims via email, websites, chat rooms, or message boards, leading to fraudulent transactions or the transfer of proceeds to financial institutions or other scheme participants. Fraudsters may gain access to online bank accounts, trick victims into transferring money, or obtain credit card information through fictitious offers (Internet Fraud, no date). With the proliferation of social media and email, digital fraud has become more prevalent, with con artists seizing new opportunities. The "Nigerian Prince" email hoax was among the first online frauds (Online Fraud, no date).

4.5 The General Responsibilities of Individuals, Governments, and Technology Companies to Protect the Privacy of Individuals

In today's digital world, privacy faces new challenges. Individuals, governments, and tech companies must protect personal information from misuse. Many people lack awareness about data sharing and cyber threats, while online platforms often collect and sell data without consent. Addressing these issues requires education, innovation, and ethical practices.

4.5.1 Responsibilities of People

The digital world presents numerous advantages and opportunities, but it also poses significant risks and challenges. Given the extensive integration of our lives with the Internet, it's crucial for people to understand how their personal data and online activities can be accessed, used, and exploited by various entities, including hackers, cybercriminals, advertisers, and governments. Individuals can take specific measures to safeguard their privacy in this digital realm, such as employing widespread encryption, limiting data access, minimizing personal information, and educating consumers about privacy policies. These actions aim to prevent privacy violations.

4.5.2 Responsibilities of Governments

In the digital age, protecting individuals' privacy depends on effective regulation. Governments must uphold fundamental human rights, including privacy, by safeguarding against arbitrary interference and breaches, particularly with advancements in technology such as artificial intelligence. They need to prevent undue interference from the private sector, third parties, and tech companies, and rely on both domestic and international laws. Legislators should regularly update privacy and data protection laws to ensure strong protection and address challenges in the technology sector (ICDPPC, 2019: 1-5). Policymakers must create context-specific laws and regulations to comprehensively protect privacy in the digital era (Allison-Hope, 2011: 3–6).

4.5.3 Responsibilities of Companies

Technology companies bear responsibility for respecting the right to privacy and must protect this right by minimizing the collection and storage of personal data. Transparency and accountability are key responsibilities of technology companies in the digital realm .

It is imperative for companies to clearly commit to protecting their users' privacy and transparently respond to lawful requests for information, implementing clear terms and standards on their platforms. When faced with government requests to process personal data conflicting with international human rights standards, companies should uphold human rights principles while safeguarding privacy. This necessitates transparency from the government regarding the legal basis for such requests (UNISCO's Report, 2021: 5) .

Technology companies should actively identify privacy risks in the digital world (Hlophe, 2023: 6_15). Companies should also specify commercially sensitive data they choose not to disclose and issue guidelines on developing artificial intelligence processes.

5. Research Findings

5.1 Violation of Privacy in the Digital World

As noted, privacy is a fundamental human right, entitling people to anonymity and control over their personal information in the digital world. However, the digital environment introduces unique risks and challenges for human rights protection. Technological advancements raise questions about whose privacy is violated and by whom or what institution. The rapid, borderless nature of the digital realm offers a new framework for both understanding and enforcing human rights, as well as for identifying new methods of privacy violations. Next, we will discuss key privacy violators.

5.1.1 Violation of Privacy by Individuals

Individuals' privacy includes personal space, family life, and protection in both real and digital worlds, with the right to choose what information they disclose. However, advancing digital services have compromised this right, leading to unintentional sharing of personal data. Such data leaves a digital footprint that can be misused, as today's actions are trackable and can be guided (Donahoe, 2014: 3).

In the modern world, many real and legitimate individuals in the digital world engage in a wide range of activities, content, and data exchange with stakeholders. It is imperative that these activities have specific legitimacy, security, and privacy measures to ensure consequences for their controllers in case of violation (Geneva meeting, 2014: 3). Therefore, the privacy of individuals in the digital world can be compromised by individuals and institutions motivated by personal, political, business, and financial issues.

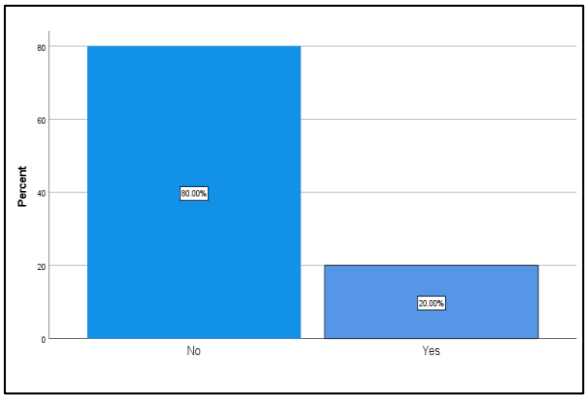
Given the extent of the Internet, users' privacy can be violated in a variety of ways, including publication or availability of private audio, video, and images; impersonation; posting personal accounts; and misuse of private information such as names, addresses, telephone numbers, etc .

Unauthorized access to computer data or communications, such as email hacking or accessing people's contacts, can result in the violation of individuals' privacy. Individuals or hackers are motivated by various reasons, including personal grievances, business interests, threats, and harassment, to violate people's privacy in the digital world. Hackers

are individuals who engage in illegal activities aimed at damaging systems and networks and stealing information.

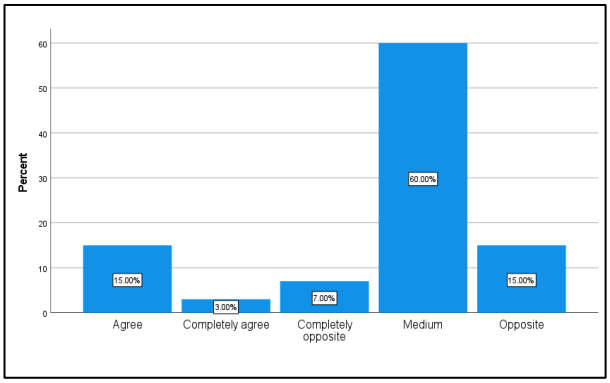
Security threats adversely affect personal information, organizations, networks, and computer systems, leading to issues like fraud, data theft, system failures, and unauthorized access to sensitive data. Online fraud illustrates privacy breaches through attempts to acquire sensitive information via fake emails, websites, or messages. Other digital privacy violations include harassment based on personal data possession. Online harassers may reveal personal details such as location, phone numbers, or workplace on social networks or public forums, causing significant distress and impacting the victim's well-being. These threats highlight the urgent need for robust privacy protection measures in the digital realm. We asked the people of Herat two questions in this discussion, which are as follows:

Question: Has your privacy ever been violated in the digital world?



In this question, we wanted to know whether their privacy was violated among the hundred respondents. 80% of the respondents chose “No”, and 20% chose “Yes”. Among 100 people, 20% of them experienced privacy violations by others, indicating that measures should be taken to protect privacy.

Question: Do you think you know enough about the risks of violating your privacy in the digital world?



Most of the time our privacy can be breached by others. In this question, we asked if respondents think they have enough information about the dangers of privacy violations, meaning how privacy may be violated by others. Respondents chose 15% "agree", 3% "completely agree", 7% "completely opposite", 60% "medium", and 15% "opposite". Most of the respondents chose the middle option, indicating they are aware of this issue, while some respondents chose the agreeing option, signifying they are knowledgeable. Similarly, the same number of respondents choose the disagreeing option, indicating they are unaware of the risks of privacy violations in the digital world.

5.1.2 Violation of Privacy by Governments

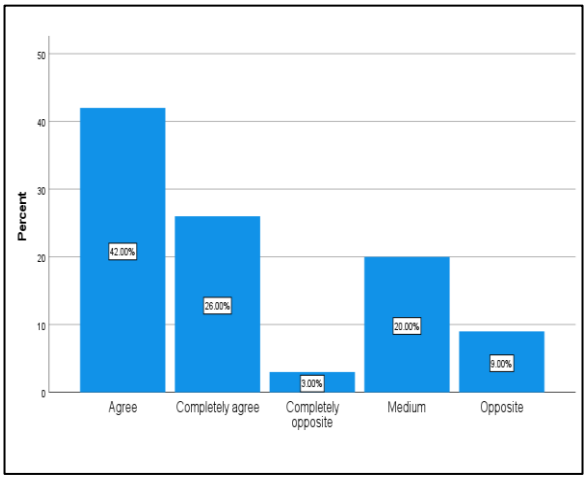
Governments are a major threat to digital privacy, often prioritizing national security over individual rights. Examples include Turkey's Twitter ban, Iran's death sentence for a Facebook post, NASA's surveillance of U.S. citizens, European rulings on Google search privacy, and China's real-name internet policy. These actions demonstrate how governments frequently infringe on privacy under the guise of national security (Donahoe, 2014: 4-5).

In June 2013, Edward Snowden exposed classified documents from the US National Security Agency, revealing global surveillance, collection, and recording of internet and phone communications by the U.S. and the UK. The "Premise Plan" demonstrated governments' significant violations of individuals' digital privacy (Amani, 2022). This discussion exemplifies several governments violating individuals' digital privacy rights. Article 37 of the Cybersecurity Act mandates storing personal data for commercial purposes and data transfers. Furthermore, under data protection laws, the Russian government requires technology partners like Google to collect and transfer personal data within Russia (Hlophe, 2023: 5).

Many national governments have blocked and restricted websites with nonviolent political, social, or religious content, prioritizing national security over privacy rights. Government surveillance and interference in individuals' privacy have reached worrying levels, with threats to telecommunications and technology companies to grant direct access for monitoring purposes. Additionally, authorities in some states record all

telephone requests for analysis (UNISCO's Report, 2021: 3-6). We wanted to understand the opinions of people in Herat on this matter, so we asked the following question：

Question: Do you think governments can breach your privacy in the digital world?



In this question, we inquired whether it is possible for governments to be involved in violating people's privacy. Respondents chose 42% for the "agree" option, 26% for the "completely agree" option, 3% for "completely opposite" option, 20% for the "medium" option, and 9% for the "opposite" option. The obtained statistics show that governments can also contribute to violations of people's privacy in the digital world, which may be considered positive and negative. For example, when governments use biometrics, they gain access to individuals' information. Thus, if someone commits a crime, they can use this information to find the culprit. This can be seen as a positive aspect if the individuals' information is securely held by the government.

5.1.3 Violation of Privacy by Technology Companies

Privacy violations are no longer limited to law enforcement and government agencies; technology giants like Facebook and Google also play a significant role. Driven by profit, they collect and record extensive personal data, including photos, voices, and political opinions. This data is often commodified and sold to other companies, making personal information a major revenue source for tech firms worldwide (Hlophe, 2023: 3).

The accumulation of data also heightens the risk of privacy infringements and data misuse. While communication and telecommunications traverse multiple servers worldwide, technology companies may inadvertently store sensitive information and compromise individuals' digital privacy. Tech and telecom service providers have access to vast amounts of user data, potentially infringing on privacy rights under lawful requests for data retention (Hlophe, 2023: 4).

The collection and safeguarding of personal data in digital technologies directly impact individuals' human rights. In an increasingly digitized world, the personal data we

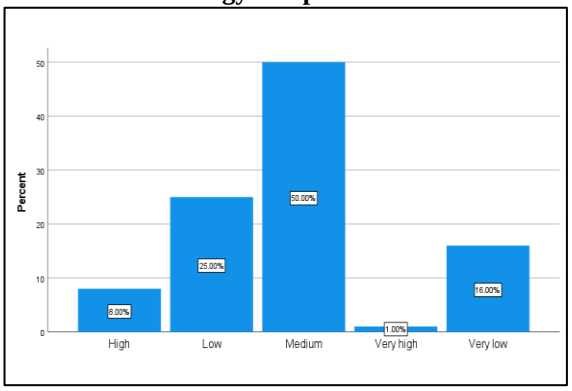
Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

share online is crucial. Consumer data obtained through digital means is utilized for targeted product marketing and other services. However, these practices also open avenues for potential misuse of personal data for nefarious purposes (Hanifan, 2020: 105–119).

While digital data collection offers significant benefits, including personalized services and targeted advertising, it must be balanced with protecting individual human rights. The importance of privacy rights cannot be overstated. Personal data, encompassing location, browsing history, and preferences, reflects an individual's identity and privacy. Unauthorized data collection, lack of transparency in data usage, and potential security breaches undermine individuals' right to control their personal information (Mardiana & Meilan, 2023: 21).

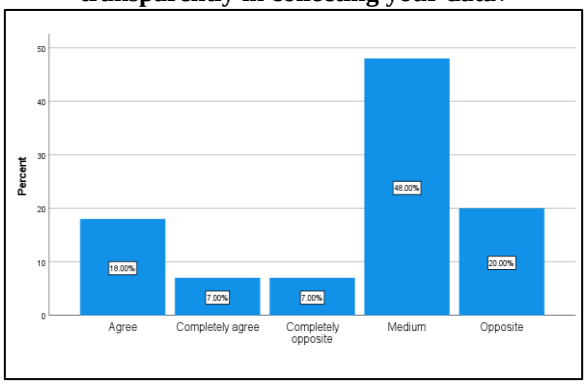
Therefore, individuals' privacy in the digital realm is compromised by various actors, including governments and technology companies driven by political, economic, and social motives. Governments are particularly susceptible to encroaching on people's privacy rights, while tech companies continuously exploit individuals' personal data. We asked people in Herat for their views on this.

Question: How much do you know about the methods of collecting your personal data by information technology companies?



Today, companies collect people's personal information for various reasons, and this large volume of personal data may be used to violate privacy. Therefore, in this question, we asked the respondents how much information they have about the way data is collected by companies. The statistics obtained from the survey show that the 8% chose the “high” option, 25% chose the “low” option, 50% chose the “medium” option, 1% chose the “very high” option, and 16% chose the “very low” option. According to these statistics, it can be concluded that people's awareness of how companies collect personal information is low, and attention should be paid to this issue.

Question: Do you think organizations and technology companies act transparently in collecting your data?



As mentioned, companies collect their customers' data for various reasons and use it for their own benefit. The question raised is whether organizations and companies act transparently in data collection. We asked the respondents about their agreement and disagreement. 18% of the respondents chose the "agree" option, 7% "completely agree", 7% "completely opposite", 48% "medium", and 20% "opposite". The most common response in this poll is the medium option

5.1.4 The Role of Artificial Intelligence in Privacy

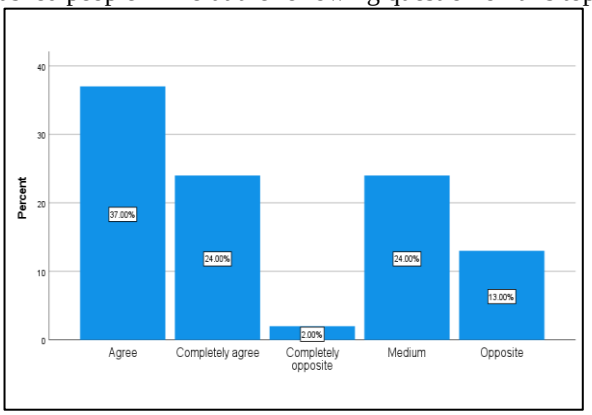
Artificial intelligence, now a key technology in daily life, offers significant benefits but also poses risks, notably regarding privacy violations. This section examines AI's role in these privacy concerns. Artificial intelligence, as a branch of computer science, creates machines that perform tasks requiring human intelligence. Research by Gerech and Fasten highlights AI's role in expanding human capabilities (Forozan, 2023: 4). AI operates on predefined rules, not observation, and is used in applications like facial recognition and self-driving vehicles.
Despite its benefits, AI can also infringe on individuals' privacy (Sam, 2023). One significant concern in modern technology is Deepfake, which can create realistic simulations of people's faces and voices (Harfield, 2021). This poses a threat to celebrities, including artists, athletes, and politicians, potentially compromising their professional lives. For instance, altering a president's speech or placing politicians in fabricated scenarios are examples of such threats.

The integration of digital technologies heightens privacy concerns, particularly with AI's role in monitoring protests and infringing on freedoms (Amani, 2022). AI's reliance on data makes it central to privacy risks, as companies like Facebook, Meta, Google, and Snapchat trade personal data for profit (Manheim & Kaplan, 2019). AI-driven targeted advertising further risks privacy by collecting extensive user data and potentially exposing sensitive information such as sexual orientation, religious beliefs, and medical history.

AI raises significant privacy concerns, particularly through tracking and surveillance. Companies like Google track user locations for various reasons, often sharing data with third parties (Rijmenam, 2023). Governments use AI tools to monitor activities on social media, restricting communication and infringing on privacy. For example,

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

Chinese companies use voice recognition software for surveillance, leading to privacy breaches and human rights abuses. Similarly, AI-driven software in China and Vietnam monitors digital communications, censoring content and leading to arrests (ICNL, 2021). The widespread adoption of AI technologies in recent years has exacerbated privacy concerns, with governments and companies leveraging AI to violate individuals' privacy rights. We asked people in Herat the following question on this topic.



Question: Do you think new technologies such as artificial intelligence will affect your privacy in the digital age?

Today, artificial intelligence is rapidly growing and has affected people's lives. Privacy is an integral part of human life and can be influenced by artificial intelligence, which people can use in positive dimensions such as privacy protection or negative dimensions such as privacy violations. Therefore, we asked the respondents whether artificial intelligence can affect privacy in the digital world. 37% of the respondents chose the “agree” option, 24% chose the “completely agree” option, 2% chose the “completely opposite” option, 24% chose the “medium” option, and 13% chose the “opposite” option. In summary, we can say that according to this poll, artificial intelligence can have an undeniable impact on privacy in the digital world.

5.2 Supporting Mechanisms on digital Privacy in the national and International Documents

The universality of human rights forms the core of international human rights law, affirming individuals' inherent rights. Privacy, crucial for human dignity, is protected by both national constitutions and international treaties, and this fundamental right to privacy and data protection must be upheld. We will examine national and international documents this right.

5.2.1 National Documents

Since 2001, the use of the internet has become widespread in Afghanistan. Over time, with the advent of new information technologies, internet use has increased, especially among the younger generation. As preserving privacy in the digital space is a crucial issue, countries worldwide have enacted laws and regulations to protect

individuals' privacy and information online. In Afghanistan, however, there is still no comprehensive law for data protection in the digital space. Nonetheless, legal experts have recognized the crime of breaching privacy in cyberspace based on the provisions of the Cybercrime Law and the Penal Code.

The Afghan Constitution of the Republic era did not explicitly protect digital privacy rights. Although the Constitution is the fundamental law from which all other laws derive, it has gaps and only addresses privacy rights in a tangible, rather than digital, context.

In 2014, Afghanistan developed a draft Cybercrime Law aimed at improving the health of the country's information systems, ensuring cybersecurity, preventing cyber incidents, and fostering international cooperation. According to this draft, cybercrimes are those committed using modern information and communication technologies in the intangible digital space (Saidi, 2020:1)

The Afghan Penal Code addresses cybersecurity and cybercrimes in Chapter Twelve. Article 851 defines cybercrimes as offenses committed using modern information, communication technology, or the internet in cyberspace. Articles 852 and 869 cover unauthorized access to computer systems and cyber extortion, specifying corresponding penalties (Criminal Code, 2017: 851).

Thus, protecting individuals' privacy is a fundamental duty of every citizen towards the state and other citizens. Anyone or any authority violating this right is acting unlawfully and should be penalized.

5.2.2 International Documents

In this section, we will examine important international documents regarding digital privacy to determine what protections have been provided for privacy in these documents .

5.2.2.1 The Universal Declaration of Human Rights (1948)

One of the largest and most important documents at the international level is the Universal Declaration of Human Rights, which is considered the basis for protecting the fundamental rights of individuals. Hence, the right to privacy is recognized by international human rights instruments for the first time. Article 12 of the Universal Declaration of Human Rights states:

"No one shall be subjected to arbitrary interference with his or her privacy, family, home, or correspondence, nor to attacks upon his or her honor and reputation." (The Universal Declaration of Human Rights, 1948: 12) According to this article, people shall not be subjected to arbitrary interference in their private lives, and they shall have the right to legal protection against such conflicts. This is stated in this article: no one shall interfere with the privacy of his or her family, relationship, correspondence, or violate his or her reputation or character as an individual. Private life has a wide scope, and everything is not related to other people's lives, so it can be considered part of private life, and family affairs are also part of personal life .

Therefore, the scope of privacy has expanded with the changes in the form of communication between individuals, and privacy includes the offline and online worlds. It can also be said that Article 12 of the Universal Declaration of Human Rights, in addition to being applicable in the real world of individuals, is also applicable in the digital

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

world of people. If someone violates the privacy of individuals without legal permission in the digital world, it includes cases under Article 12 of the Universal Declaration of Human Rights.

5.2.2.2 International Covenant on Civil and Political Rights (1966)

The International Covenant on Civil and Political Rights is the only one document that explicitly states regarding the privacy of individual

According to Article 17 of the International Covenant on Civil and Political Rights, the privacy of individuals is accepted and protected, so this article elucidates under two clauses: No one shall be subject to arbitrary or unlawful interference with his private, family, residence, or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to be protected by the law against such interference or attacks (International Covenant on Civil and Political Rights, 1966: 17).

According to the first paragraph of this article, people have the right to protection in their private life, family, home, or relationships, and no one has the right to interfere arbitrarily, without reason or illegally with their privacy, or hurt their reputation and status. Also, pursuant to the second paragraph, anyone who encounters invasions and damages to their privacy has legal protections. This clause states that there should be protections and permissions against any possible interferences and damages to the privacy of individuals (Josef &Schultz, 2000: 348) .

5.2.2.3 Other Documents

In addition to the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, several key documents affirm privacy as a fundamental right. Regional conventions, such as Article 11 of the American Convention on Human Rights and Article 8 of the European Convention, reinforce privacy protections (Damen et al., 2017). Since 2013, the UN General Assembly and the Human Rights Council have issued resolutions on digital privacy. The September 2019 resolution highlights that any interference with privacy must follow legal principles of necessity and proportionality, ensuring online rights match offline rights (International Standards OHCHR, no date). Furthermore, the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC), held in October 2019 in Tirana, established an international resolution recognizing privacy as a fundamental human right essential for the exercise of other rights (ICDPPC, 2019).

At the end, it would be good to discuss exceptions to interference in the privacy of individuals according to the law. However, the right to privacy is restricted by certain laws in certain circumstances for specific reasons. While the right to privacy is not absolute, any limitation to it must be provided for by law. This means that the law should be sufficiently clear, precise, and accessible because people can comply with it and specify who and under what conditions may be authorized to monitor the data, so the rules in general, especially in respect of privacy, should be legal, appropriate, and compatible with other human rights (Geneva meeting, 2014: 2).

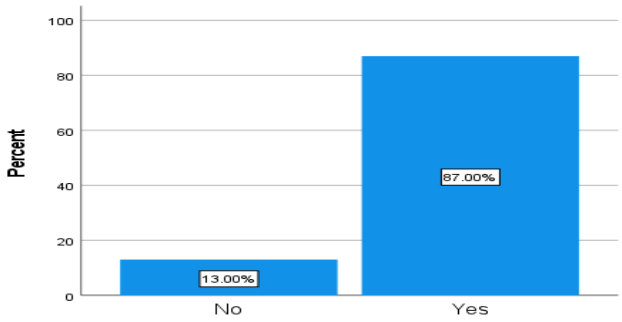
Therefore, there must be a legal human rights reason why governments, law enforcement agencies, and companies are allowed access to personal information. This is why it is possible for law enforcement organizations to access the data (Allison-Hope, 2011: 5_7).

5.3 People's perspectives on The Responsibility of Individuals, Governments, and Technology Companies to Protect the Privacy of Individuals in Herat Province

Digital privacy has become one of the most significant contemporary issues in the realm of technology and communication. With the rapid expansion of digital technologies and online spaces, the protection of personal information and data confidentiality has gained paramount importance. In Herat, where technological advancements and the number of internet users are growing swiftly, concerns about digital privacy have become a critical issue. This matter encompasses the roles and responsibilities of individuals, companies, and the government in safeguarding and securing citizens' private information. This section of the research will examine various people's perspectives on the responsibilities of companies, individuals, and governments.

5.3.1 Responsibilities of People

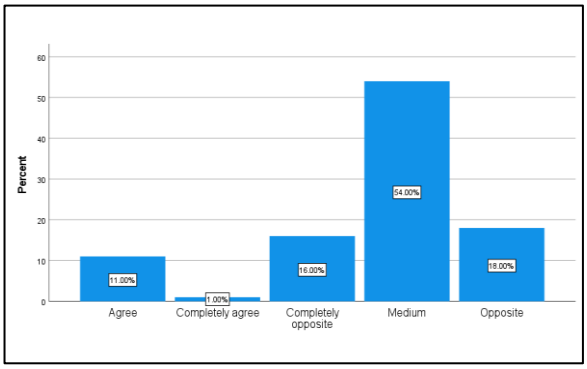
Protecting digital privacy is the responsibility of each individual. By using strong passwords, security settings, and limiting information sharing, one can prevent potential misuse and safeguard their privacy. We asked the people of Herat: Have you ever used tools and methods such as encryption and updating to protect your privacy in the digital world?



In this question, we asked the respondents if they use encryption and update old applications to protect their privacy. According to the available statistics, 87% of the respondents chose the "Yes" option, and only 13% chose the "No" option. This statistic makes us optimistic that people pay attention to protecting their privacy so that it is not violated by other.

5.3.2 Responsibilities of the Government of Afghanistan

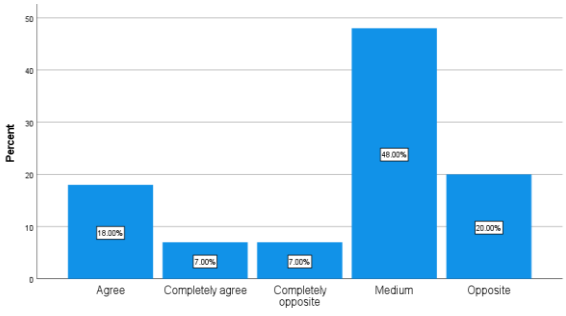
The responsibility of the Afghan government for protecting digital privacy includes establishing and enforcing effective laws to safeguard personal data, overseeing cybersecurity, and strengthening digital infrastructure. The government should provide necessary training to raise public awareness and establish mechanisms to address privacy violations. We asked the people in Herat: Do you think there is a sufficient guarantee of enforcement at the international and national rules against violating your privacy in the digital world?



When crimes occur in the digital realm, it is essential to have both national and international enforcement mechanisms to deter such activities and ensure perpetrators are held accountable. In this question, respondents were asked about their perception of enforcement guarantees against privacy violations at these levels. The options and corresponding percentages were as follows: 11% selected "agree", 1% chose "completely agree", 16% opted "completely opposite", 54% indicated "medium", and 18% selected "opposite". These results indicate that respondents believe there is insufficient enforcement guarantee against privacy violations in the digital world. This perceived the lack of enforcement may contribute to the prevalence of online crimes.

5.3.3 Responsibilities of Companies in Afghanistan

Companies' responsibility for protecting digital privacy includes implementing robust security measures, complying with privacy regulations, and being transparent about data collection and use. They must regularly update their systems, inform users about how their data is used, and take steps to protect data against cybersecurity threats. We asked the people of Herat: Do you think organizations and technology companies act transparently in collecting your data?



As mentioned, companies collect their customers' data for various reasons and use it for their own benefit. The question raised is whether organizations and companies act transparently in data collection. We asked the respondents about their agreement and disagreement. 18% of the respondents chose the "agree" option, 7% "completely agree",

7% “completely opposite”, 48% “medium”, and 20% “opposite”. The most common response in this poll is the medium option.

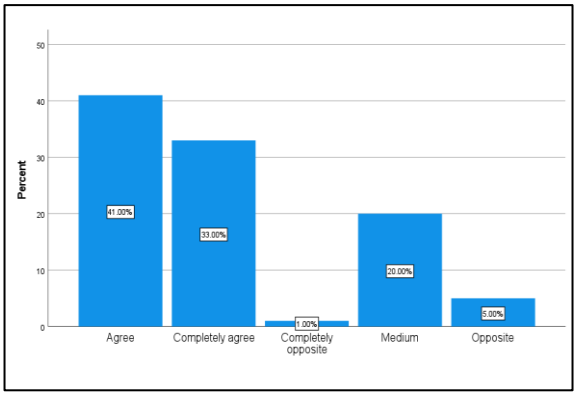
5.4 Consequences of Digital Privacy Violations

Online privacy is deeply rooted in our basic security needs. While protecting individual privacy is crucial, the technical, legal, commercial, and social complexities of today’s age have made it challenging. Violations of individuals' privacy can have far-reaching consequences for various aspects of human existence, as we will address in this section (What is online privacy?, no date).

5.4.1 Violating the Security of Personal Information

Online privacy is intertwined with every aspect of our lives. Governments may seek to exert control over us by accessing our personal information. When our personal data is in the hands of individuals, companies, and governments, it can be vulnerable to various security risks. Particularly when this information falls into the wrong hands, it can be exploited for malicious purposes. Privacy directly impacts the security of our personal information and can have a positive effect on our overall security (The importance of data privacy, 2023). We asked people in Herat the following question on this issue .

Question: Do you think that by violating your privacy in the digital world, your personal data will be misused?



In today’s digital age, the violation of privacy and misuse of personal information are widespread concerns. In the survey, respondents were asked whether privacy violation lead to the misuse of personal information. The respondents chose 41% for the “agree” option, 3% for the “completely agree” option, 1% for the “completely disagree” option, 20% for the “medium” option, and 5% for the “disagree” option. Based on these this statistics, it can be inferred that privacy violations in the digital world may indeed lead to misuse of personal information, including photos.

5.4.2 Violating Financial Security

We live in a world where there is intense competition for wealth. While some people strive to earn money through legal means and fulfill their responsibilities, others resort to illegal methods. We aim to avoid giving scammers the opportunity to misuse our personal

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

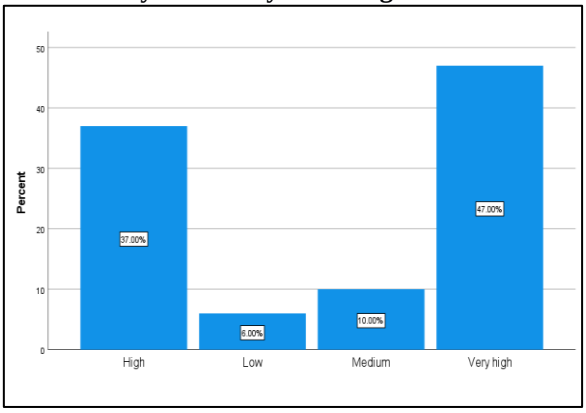
information, such as our date of birth. If someone gains access to our financial information or social security numbers, they could potentially open credit card accounts in our name, commit identity theft, and impersonate us, leading to serious consequences.

5.4.3 Violating Psychological Security

When our privacy is compromised, it poses a threat to our mental health, leading to stress, anxiety, and feelings of vulnerability. For instance, geolocation programs track our location, creating a sense of observation and monitoring, which can cause discomfort and paranoia, ultimately impacting mental health (The psychological impact of geolocation app privacy violations, 2023).

According to counseling psychologist Namrata Khetan, constant invasion of privacy encroaches on personal space and security, resulting in paranoia, fear, uncertainty, and hypervigilance. These factors collectively diminish trust in people, surroundings, and environments. A study as early as 2011 found a link between increased stress, anxiety, and fatigue and surveillance. We asked people in Herat the following question about this discussion.

Question: How much the protection of privacy can help you to reduce your anxiety and worry in the digital world?



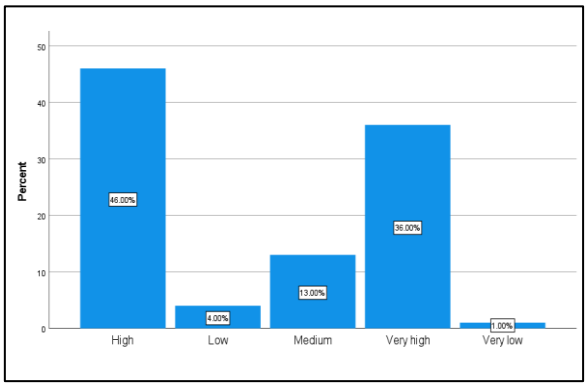
We live in an era where technology has become an inseparable part of our lives. People rely on the digital world to solve problems and conduct work online. Privacy violation poses a significant challenge, leading to constant worry about potential disclosure or misuse of important information. In this question, respondents were asked how much privacy protection helps in reducing their anxiety. 37 % chose the “high” option, 6% selected “low” option, 10% opted for “medium” option, 47% indicated “very high” option, and 0% chose “very low” option. These results show that one of the consequences of privacy protection is a reduction in anxiety and concern in the digital world.

5.4.4 Violating Social Security

One consequence of the virtual world is its impact on people's social standing, which can be negative. Violating the privacy of one's social space puts individuals at risk, while

preserving their privacy enhances their social standing. For instance, disclosing personal information, which is considered private, can significantly damage individuals' social status within society, leaving a lasting impact on people's perceptions. Imagine if a social app like Facebook were hacked, and the hacker sent immoral messages or photos to different people in your name through your account. Such incidents can have detrimental consequences for individuals. We asked people in Herat the following question on this issue.

Question: How much the protection of your privacy can affect your social security in the digital age?



protecting social security in society is crucial as people aspire to live peacefully and securely in their social lives. Privacy violation lead to breaches in people's social security. In this research, respondents indicated their preferences: 46% chose the “high” option, 4% the “low” option, 13% the “medium” option, 36% the “very high” option, and 1% the “very low” option. These statistics highlight the direct correlation between maintaining privacy and upholding the social security of individuals.

6. Conclusion

Despite the long-standing history of privacy, after centuries, privacy holds a special place in the national, international, and customary laws of society. With the digitalization of people's communications in this era, the issue of the right to privacy has emerged in the digital world, carrying a significance akin to real-world communication. However, there are several problems regarding the protection of privacy. Accessing personal territory that one wishes to be protected from others in the digital world often leads to the violation of this privacy. In today's world, there is still no flexible interpretation of the concept of privacy, and the modern world lacks the understanding that individuals should have the right to privacy in the digital world as they do in the real world.

The privacy of individuals in the digital world can be breached by various entities, including governments, technology companies, and individuals themselves. Individuals may compromise privacy due to a lack of information regarding their digital privacy or the unreliability of virtual programs. Publishing and broadcasting sensitive personal information are among the reasons that lead to privacy violations. Today's world, with the expansion of modern technologies, brings both important values and achievements, but also violations of human rights in the online world. Artificial intelligence, in particular,

Taj Academic and Research Journal ◇ Vol 1 ◇ Issue 2 ◇ 2024

poses a significant challenge to privacy rights by processing large amounts of personal data. The increasing development of digital technologies has further led to the erosion of people's privacy. Privacy challenges have become more complex with advances in artificial intelligence.

Governments and technology companies are known to be among the violators of privacy in the digital world. Governments often justify privacy violations in the name of national security, while technology companies collect and misuse personal data without proper consent or transparency. Privacy violation can also lead to personal, financial and psychological consequences .

Although the right to privacy is recognized in national and international documents, but countries including Afghanistan, have not explicitly recognized this right being practiced in their domestic rules of laws.

Ultimately, the protection of personal data to ensure the security of personal data as a fulfillment of privacy rights in today's society is not currently optimally implemented.

7. Suggestions

1. Government of Afghanistan should recognize privacy as a fundamental and vital human right to safeguard other democratic rights, including the integration of democratic processes, and should provide legal guarantees and support to prevent intrusion, manipulation, obscuration, or discrimination in privacy, especially in light of the development of new technologies such as artificial intelligence.
2. Legislators should review and update privacy and data protection laws to ensure they offer robust protection, meaningful damages, and tangible solutions in global political and technological circles.
3. The media and human rights organizations should create training programs to educate and inform people, advising against accessing non-public websites and exposed networks without warning.
4. At the international level, human rights defenders should establish special commissions or agencies to handle complaints of privacy violations in the digital world, investigating and ensuring severe enforcement.
5. Individuals should strive to raise their awareness of privacy protection in the digital world, which is their human right. Therefore, individuals must adhere to privacy practices.
6. Companies must ensure the security of their customers' information.

8. References

Books and Articles

1. Adrienn, Lukacs (2016). **What is privacy? The History and Definition of Privacy**, Publishing: Core

2. Allison-Hope, Dunstan, (2011) **Protecting Human Rights in the Digital Age, Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry:** BSR Report Publishing .

3. Amani, Elahe (2022). **Privacy in the Virtual Space and gender**: Asre Publishing.

4. Arbani, Elham, Vahedi, Mehdi (2019) **Privacy of Users in Cyberspace in Order to Provide Solutions for its Preservation:** University of Allameh Tabataba'i.
5. Damen, Juliane & Köhler, Lena &, Woodard, Sean (2017). **"The Human Right of Privacy in the Digital Age":** Potsdam University Press Publishing.
6. Donahoe, Eileen (2014) **Human Rights in the Digital Age: Just Security**.
7. Fathi, Younis & Shahmoradi, Khirollah (2017). **Wide scope and domain of privacy in the digital space**: Dadgostary Publishing.
8. Forozan, Amir Reza, (2023) **How Can Artificial Intelligence Threaten our Privacy and Identity?** Publishing: Digiato
9. Gauri, Pandey (2023) **Online Harassment in Digital Age- Combating the Issue with Lagal Provisions** .
10. Hanifan, Niffari (2020**). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi** (Suatu Tinjauan Komparatif Dengan Peraturan Perundang- Undangan Di Negara Lain: Journal Yuridis .
11. Harfield, Jake (2021**). Is AI Dangerous? 5 Immediate Risks of Artificial Intelligence**.
12. Hlophe, Nolwazi (2023). **Data Privacy in the Digital Era: Are Human Rights at Risk**?
13. Josef, Sarah & Schultz, Jenny (2000). **The international covenant on Civil and Political rights, Cases, Materials and Commentary**: Oxford University Publishing
14. Joyce, Daniel (2015) **"Privacy in the Digital Era: Human Rights Online**."
15. Khatri, Mousam (2023) **Cyber Bulling: Unmasking the dark side of the digital**.
16. Manheim, Karl & Kaplan, Lyric (2019) **Artificial Intelligence: Risks to Privacy and Democracy,** The Yale Journal of Law & Technology Publishing.
17. Mardiana, Nela & Meilan, A (2023). **Urgensi Perlindungan Data Pribadi Dalam Perspektif Hak Asasi Manusia,** jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia .
18. Rijmenam, Mark Van (2023). **Privacy in the Age of AI: Risks, Challenges and Solutions**.
19. Sam, Noss, (2023**). Generative AI and Its Impact on Privacy Issues**.
20. Saidi, Mostafa (2020). Cyber Crimes in Afghanistan and Legal Provisions.
21. Siagian, Riduan &, Siahaan, Eonard& Hamzahs, Muhammad Ichwan (2023). **"Human Rights in the Digital Era: Online Privacy, Freedom of Speech, and Personal Data Protection":** Journal of Digital Learningand Distance Education Publishing.
22. Zamboni, Alessandro, & Gérôme, Bilis & Raphaël, Brun& Youri Dufau, Sansot (2016) **Privacy in the Digital World: Beyond Compliance, Towards Trust:** www.wavestone.com publishing .

Cites

1. **Biggest Hacks of 2023 understanding where to improve** (2023), Available: https://www.keytos.io/blog/cloud-security/biggest-hacks-of2023
2. ICNL (2021) **The impact of Artificial Intelligence Technologies on the Right to Privacy and Civil Freedoms**.
3. Internet Fraud(no date), Available: www.afp.gov.au

4. **Online Fraud,** Available https://www.fraudsmart.ie/personal/fraud-scams/online-fraud/
5. **The importance of data privacy in the digital age** (2023), Available https://www.linkedin.com/pulse/importance-data-privacy-digital-age-thetechmarketer
6. **The psychological impact of geolocation app privacy violations** (2023), Available https://utilitiesone.com/the-psychological-impact-of-geolocation-app-privacy-violations
7. **What is online privacy? And why is it important?** Available https://www.bitdefender.com/cyberpedia/what-is-online-privacy/

National and International codes, documents and Reports

1. Criminal Code of Afghanistan, 2017 .
2. Geneva meeting (2014) The right to Privacy in the Digital Age: Meeting Report .
3. International Covenant on Civil and Political Rights.(۱۹۶۶)
4. International Standards OHCHR, (no date) Privacy in Digital age, United Nations, Human Rights, Office of the Commissioner .
5. ICDPPC, International Resolution On Privacy AS A Fundamental Human Rights und International Precondition for Exercising Other Fundamental Rights ,41st International Conference of Data Protection and Privacy Commissioners, 2019, Tirana, Albania
6. The Universal Declaration of Human Rights.(۱۹۴۸)
7. UNISCO's Report (2021) A/HRC/27/37, The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights, United Nations.