

Digital Privacy and Security in Wartime: Examining Societal Trends and the Impact of Social Media Platform Policies during the 2023 Gaza War

Tahreer Isbeetan¹, Abdallah Adway² 

Arab American University¹, Global Digital Academy²
Corresponding author: tahreer.isbeetan@gmail.com

DOI: <https://doi.org/10.67732/jidmc.v1i1.8>

Abstract

This study aims to analyse the level of awareness of digital privacy and security in Palestinian society, the perceptions and concerns of users of digital platforms after the outbreak of the war on Gaza in October 2023, and the policies of social media platforms regarding digital activity, as well as the impact of these policies on users' behaviour, interaction and digital practices during the war. The study used a quantitative approach, relying on a questionnaire. The study concluded that the level of awareness of digital privacy among citizens in Palestinian society is average at 60.7%, reflecting awareness of the importance of preserving personal data and the risks of disclosing it in digital environments, which leaves a high percentage of society vulnerable to misleading information, such as fake links. The study also concluded that the perceptions of users of digital platforms reached 60.4%, which is also an average degree towards security and digital risks. The study concluded that the level of impact of social media policies on the activity of the Palestinian digital society after the war came to an average degree of 61.7%.

Article History

Received 19-06-2026
Accepted 27-06-2026
Published 10-07-2026

Keywords

Privacy, Digital Security, Social Media Platforms, Gaza War 2023.

Introduction

Digital privacy and security are among the basic rights guaranteed by international conventions, such as the European Convention (Council of Europe, 2004) on Data Protection, the Budapest Convention on Combating Cybercrime (2001) and the Arab Convention on Combating Information Technology Crimes (2010), all of which stressed the need to strengthen international cooperation to confront cybercrime and ensure the protection of individuals in the digital environment. Recent studies have also (Sulaimani, 2023) indicated that technical development has forced a review of national legislation to ensure a balance between national security requirements and individual privacy rights.

In the Palestinian context, the issue of digital privacy and security has taken on a particular dimension since the war of October 7, 2023, when the Palestinian digital space (Graff, 2023; Abu Arqoub, 2021) has been subjected to systematic violations, including electronic censorship, content blocking, and the targeting of activists on social media networks. These events have exposed the fragility of digital security and the inadequacy of protective tools for Palestinian users, as reflected in the level of

digital political participation, especially given the media and cyber conflict parallel to the military aggression.

The importance of the study lies in addressing a topic related to privacy and digital security, which is one of the issues facing Palestinian society amid the difficulties and challenges of the current situation, especially considering the Palestinian reality after the events of the 7th of October 2023 war. It contributes to enriching scientific knowledge. Therefore, this study is considered a scientific addition to digital media research in the Palestinian reality. It enriches the library with new, continuous literature for analysing the relationship between privacy and digital security in the Palestinian reality.

This study aims to analyse the level of awareness of digital privacy and security in the Palestinian society, and to understand the perceptions and concerns of users of digital platforms after the October 7, 2023 war, as well as to analyse the policies of social media platforms on digital activity, and the reflection of these policies on users' behaviour, interaction and digital practices during the war.

Literature Review

Many studies have examined digital privacy, its dimensions, risks, and forms of infringement, and there are numerous definitions of digital privacy. A study confirmed (Moussaoui, 2022) that it is difficult to define an accurate concept of the right to digital privacy, given the continuous and accelerating technical development the world is witnessing today. It also looked (Al-Sharif, 2022) for the concept of the right to privacy in general, and to identify the concept of digital privacy in particular, considering a digital society in which there is a form of safe and instant interaction.

The previous studies also dealt with the digital privacy policy of social networking sites as a study, (Shaalal, 2022) which clarified the responsibility for violating it, whether the responsibility of social networking sites themselves or the responsibility of their users, as well as the responsibility of the state and the judicial system.

The studies by Dahmani & Jaraya (2022) and Faqiha (2022) explained the most important challenges facing digital privacy. However, the study by Dahmani & Jaraya (2022) examined these challenges worldwide during the COVID-19 pandemic, confirming that digital privacy is significantly violated and threatened. It also highlighted the difficult challenges, especially in the context of crises. It showed that governments and intelligence agencies are among the top threats to digital privacy and personal information, which puts them in a difficult position in balancing privacy and security. Accordingly, the researcher recommended taking preventive measures to ensure digital security and obliging technology companies, application developers, and the phone industry to ensure the safety of basic systems and users' personal data.

As for the study of (Faqiha, 2022), it revealed that Internet users in the digital age are exposed to digital privacy issues, and that few Internet users are aware of the violation of privacy. It agreed with (Dahmani & Jaraya 2022) that institutions, governments and Internet users all face digital privacy challenges, and are vulnerable to security violations. However, it indicated that the future of digital privacy changes from time to time, and that there should be more interventions in protecting digital data, such as

e-mail and malware, and that the forensic analysis of digital networks should be carried out, which contributes to reducing digital privacy problems.

The study of (Xu & Others 2020) touched on a different aspect of digital privacy and digital security, which is the medical field, explaining that the policy of the mobile smart medical network leads to making it more vulnerable to security threats as it damages digital privacy and security, and works to leak privacy compared to traditional wired networks, indicating that its proposal to create a system for data security and digital privacy protection fits the scenarios of mobile smart medical applications, which contributes effectively to data security and user privacy.

A similar study (Awad, 2021) confirmed that the threats of cyberattacks may lead to paralysis of medical technical systems and harm them. It revealed that legal legislation is not only the one that can preserve the privacy of digital individuals, but also ensures its application and amenability, based on the latest developments in violations affecting digital privacy, as well as the application of policies on an ongoing basis to ensure the protection of digital privacy.

In another context, some studies such as (Buchan, 2023) and (Rizk & Cordey 2023) addressed the risks (Ndlovu, 2023) and concerns of digital privacy. The study (Buchan, 2023) revealed the deep risks to the right to privacy and data protection in contemporary wars. The study also showed that technological advances in the fields of electronic surveillance, predictive algorithms, big data analytics, user generated evidence, artificial intelligence, cloud storage, facial recognition, and encryption redefine the scope, nature, and features of military operations. In contrast, international humanitarian law provides very few, if any, rules of private law related to the legal processing, analysis, dissemination, and retention of personal information.

While the (Ndlovu, 2023) study revealed concerns related to online privacy from pesky security compromises such as targeted ads to leaks that have an impact on private affairs, stressing that they are related to tracking when browsing the Internet, where many find that targeted ads are intrusive, in addition to theft, where identity theft is a serious problem that is fairly widespread online, and cybercriminals infiltrate accounts, computers, and phones using viruses, spyware, and phishing methods to obtain private information to be used in identity theft. The study emphasized that enhanced intelligence sharing, coordination of cyber defines tactics, and enhanced response capabilities can improve data security procedures by providing immutable logs, flaw detection, and prediction of potential attacks.

While the study of (Rizk & Cordey 2023) showed that there are three types of digital risks in times of conflict, including those related to humanitarian actors of digital technology to support humanitarian and protection activities, including those related to the use of armed actors to support military operations such as information and cyber operations against civilians, or infrastructure, or the misuse of personal and humanitarian data, including those related to the reuse of technologies and infrastructure, or the dual use of them, and allows the involvement of civilians in conflict-related actions, such as surveillance, intelligence gathering or cyber and information operations.

The study of (Khadam & Others 2020) also showed that many attempts have been made to meet the requirements of Internet users to protect their privacy and digital security. However, major risks arise related to digital privacy and security policy. The study also showed that digital documents and copyright protection are important issues in the Internet of Things, according to the fact that they are distributed, reproduced and disclosed by communication technologies on a large scale, and verifying and certifying the ownership of digital documents is necessary.

Previous studies dealt with digital security and awareness of digital privacy, especially among university students, including the study of (Al Sayed & Sayed 2022), which focused on the values of enhancing digital security among university students in Egypt and showed that it is available to a medium degree, and that intensive efforts are needed to introduce it and its importance. It recommended the need to develop and strengthen to meet the challenges of the digital revolution, through some of the proposed practices and procedural mechanisms.

In the same context, the study of (Mahajer & Nouari 2022) focused on knowing how Facebook users deal with topics related to information privacy, and addressed the forms of violations to which users are exposed through social media networks, and how they deal with the data of others, stressing that dealing with personal data is linked to some variables and factors such as age, gender, and cultural and social standards, and recommended the need to spread legal awareness among users of social media networks regarding the importance of the right to digital privacy, and the need to be aware of the policies governing the functioning of websites and applications by reviewing them in advance before registering within them. As for the study of (Rajab & Others 2023), it also looked at the awareness of digital privacy among users of new media, explaining that the cognitive aspect of awareness of digital privacy is medium, while the emotional aspect is weak, as well as the level of skill aspect of the sample.

In the Palestinian context, a study shed (Abu Arqoub, 2021) light on the reality of digital privacy in Palestine and the repeated Israeli violations against it before the war on Gaza in 2023, which reveals a research gap in the Palestinian reality in light of the 2023 war, despite the importance of digital privacy and security at this particular time. (Adway, 2023)

The study by Othman (2025) revealed the increasing challenges posed by digital development and facial recognition technology, which can lead to arrests. It also highlighted the gap between legal frameworks and the rapid pace of digital development, indicating that the right to privacy lacks a legal foundation.

Similarly, the study by Husary (2025) examined the freedom of digital narrative and the challenges facing Palestinian users in the digital age. The study emphasized the double standards exhibited by social media platforms, where Palestinian content is subjected to restrictions. It also indicated a desire among Palestinian users for fairness regarding digital privacy.

Meanwhile, the study by Al-Masaeed (2025) explored privacy in the digital age between theory and practice considering international standards. It also examined the specific Palestinian national systems related to digital privacy, the right to choose how

to ensure privacy protection for Palestinians in the digital age, and the systematic use of these systems by the Israeli occupation as a pretext for exploiting Palestinians' digital rights. While the study (Ibn Amra, 2024) explained the digital transformation and its impact on privacy, it revealed several threats and challenges that digital transformations pose to individuals' rights to digital privacy, and it clarified the effective and sufficient guarantees for protecting digital privacy.

The October 7, 2023, war, known as the "Al-Aqsa Flood" represents a critical turning point in Palestinian political and digital histories, revealing new dimensions of Israeli cyber hegemony over the Palestinian cyberspace, and the scale of violations of the privacy and digital security of individuals and institutions.

Since that day, the Palestinian digital environment has become a parallel arena for field warfare, in which Israel uses artificial intelligence tools, espionage systems, and content restrictions to undermine Palestinian collective awareness and control the flow of information (Human Rights Watch, 2024).

Reports showed that the Israeli occupation employed specialized intelligence units, most notably Unit 8200, to expand the scope of digital surveillance and collect big data about Palestinians, taking advantage of technical capabilities in analysing behaviour and communication patterns, which made every smart device or electronic account a potential target for surveillance (Al Jazeera, 2021). The use of AI technologies such as the Lavand R system to automatically identify human targets has been documented, resulting in civilians being targeted based on inaccurate algorithms (Ifex, 2025).

Field reports also showed that violations of digital privacy escalated in an unprecedented way after the outbreak of the war, as thousands of Palestinian posts were deleted from social media platforms, news and influential accounts were closed under the pretext of "breaching standards," while Israeli content was overlooked even when it included incitement or justification for violence. (Sulaimani, 2023)

A report issued by the Arab Centre for the Development of social media "Campaign" confirmed that these policies created an "unfair digital system" that reproduces Israeli control within cyberspace. (The Arab Center for Social Media Advancement, 2024)

The Israeli "coordinator" application has also become a central tool in the digital occupation system, collecting data of Palestinian users under the pretext of "civil services", while information is used for intelligence and permanent monitoring purposes (Quds Network, 2020). This reflects what can be described as ' soft security engineering ', which seeks to manage Palestinian society via data rather than direct field management.

The October 7 war was not just a military confrontation, but a moment in which all dimensions of digital colonialism intensified, as cyberspace turned into a field of cognitive and political warfare, in which surveillance and repression are practiced through algorithms, and data is weaponized as a new weapon against Palestinian awareness. Therefore, the researcher believes that understanding the effects of this war on privacy and digital security is a condition for understanding the nature of

transformations in Palestinian digital sovereignty, and for identifying ways to promote digital resistance as one of the tools of national liberation.

Methodology

The study used the quantitative approach, based on the questionnaire tool. This study is considered a descriptive study as it seeks to describe and classify facts and data.

The study population consists of citizens of the State of Palestine, and the population was estimated at 5.5 million, including 2.8 million males and 2.7 million females, in addition to about 1.9 million Palestinians residing in the lands of 1948, in the West Bank (3.43 million), the Gaza Strip (2.13 million), and the population of East Jerusalem (1.86 million) (Palestinian Statistics Centre, 2025) in order to learn their views on digital privacy in light of the war on Gaza, and its impact on their digital political participation.

The researcher relied on the simple random sample, which is the sample in which all elements of society have equal opportunities (Masoudi, 2022), through the distribution of the electronic questionnaire to the study sample consisting of male and female citizens in the Palestinian society in each of (the West Bank, the Gaza Strip, Jerusalem, and the occupied interior), which amounts to (500) male and female citizens, based on the statistical bases to determine the sample in large communities according to the Cochran's Equation, as a sample of 384 citizens is sufficient at a level of confidence of 95% and a margin of error of 5%.

Quantitative data were analysed by the Statistical Packages for the Social Sciences (SPSS) program, using arithmetic averages, standard deviations, and percentages.

The stability coefficient (Cronbach Alpha), which measures the stability of the tool, reached (91%), which is a high percentage indicating the stability of the tool.

Findings

The study used arithmetic averages, standard deviation, and percentages to answer the study question and achieve its objectives. The results in Table (1) revealed the level of awareness of digital privacy among citizens in Palestinian society.

Table 1

The level of awareness of digital privacy among citizens in Palestinian society

Item	Mean	Standard Deviation	Percentage (%)	Level
Clearly understand what is meant by digital privacy	3.3139	1.27082	66.278	Moderate
I have prior knowledge of digital privacy	2.8511	1.09340	57.022	Moderate
I understand the importance of maintaining my personal data in digital platforms	2.9859	1.17456	59.718	Moderate
Check out my privacy policies before I use any digital platform like Facebook, Instagram, ...	3.0301	1.17189	60.602	Moderate

I understand the risks of disclosing my personal data in digital platforms	3.1107	1.18706	62.214	Moderate
I am cautious about unclear information such as links, fake plugins and anonymous or vague messages	2.9558	1.14627	59.116	Moderate
I have basic knowledge of the methods available to protect my digital accounts	3.0302	1.15168	60.604	Moderate
I know that there are laws and legislation that protect digital privacy	3.0605	1.15836	61.21	Moderate
I believe that awareness of digital privacy is very important during the recent war on Gaza	3.0141	1.11092	60.282	Moderate
Total	3.0391	1.1627	60.7	Moderate

It is clear from the previous table that the total response to the axis of awareness of digital privacy among citizens in Palestinian society is (60.7%), with an arithmetic average of (3.0391).

The results show that the highest response was "clearly understood what is meant by digital privacy", at 66.2%, while the lowest response was "I have prior knowledge of the issue of digital privacy" at 57%.

The results of the quantitative study indicate that levels of awareness of digital privacy vary among citizens and are insufficient to protect them from digital violations.

The study also analysed the perceptions of users of digital platforms in the Palestinian society about digital safety considering the war on Gaza, see Table 2.

Table 2

Digital platform users' perceptions in Palestinian society of digital security considering the war on Gaza

Item	Mean	Standard Deviation	Percentage (%)	Level
The use of digital platforms considering the war on Gaza was considered unsafe	3.4637	1.20550	69.274	Moderate
The war has increased digital and security risks for users of Palestinian digital platforms	2.9920	1.13944	59.84	Moderate
I feel that a large part of the digital information of Palestinian citizens is vulnerable to Israeli access during the war	2.9960	1.21150	59.92	Moderate
The war was a motive for Israel to increase the penetration of Palestinian accounts without pretexts	3.0664	1.14899	61.328	Moderate

I believe that digital security in Palestine is subject to digital repression, and threats by multiple parties	3.0483	1.15077	60.966	Moderate
I understand that the Israeli occupation authorities use surveillance and tracking technologies to spy on the personal data of the Palestinian user	2.9475	1.17380	58.95	Moderate
I understand that privacy laws in cyberspace are sufficient to protect and prevent exposure to information theft and access to digital security	2.8853	1.17643	57.706	Moderate
I understand that the digital culture in the Palestinian society is insufficient to protect the citizen from exposure to information theft and access to digital security	2.7827	1.22518	55.654	Moderate
Total	3.0227	1.1789	60.4	Moderate

It is clear from the previous table that the perceptions of users of digital platforms in the Palestinian society about digital security considering the war on Gaza came to an average degree (60.4%), with an arithmetic average of (3.022).

The highest response was "I consider the use of digital platforms in light of the war on Gaza unsafe" (69.2%) while the lowest response was "I realize that the digital culture in Palestinian society is sufficient to protect the citizen from exposure to information theft and access to digital security" (55.6%).

The reality of digital privacy in Palestine is weak and complex due to the control of the occupation over the telecommunications and Internet infrastructure, in addition to the exploitation of users' data by major companies for political and commercial purposes, and the absence of legislation and regulations in conjunction with the varying awareness of users of the risks of digital privacy and protection methods.

The results of the study also revealed concerns about digital privacy, during the October 7, 2023, war.

Table 3

Digital privacy concerns during October 7, 2023, war

Item	Mean	Standard Deviation	Percentage (%)	Level
I am afraid to use interactive icons (like it, like it, irritate me, grieve me, etc.) on any posts supporting Gaza and its resistance	3.0626	1.19962	61.252	Moderate

I am afraid to comment on any post related to the war on Gaza for fear of being arrested	3.0926	1.14805	61.852	Moderate
I am afraid to share any post related to the flood of Al-Aqsa for fear of being arrested	3.1109	1.15374	62.218	Moderate
I am afraid to follow news pages related to the flood of Al-Aqsa because of the fear of prosecution and arrest	3.0648	1.14464	61.296	Moderate
I have concerns about the exploitation of my personal information and news from the Israeli side	3.1851	1.13501	63.702	Moderate
I fear Israeli persecution because of supporting Gaza and resistance through digital platforms	3.1290	1.13328	62.58	Moderate
I am concerned about the theft of my account and the publication of what is not appropriate in it, as happened with many prisoners by publishing the phrase (I love Israel)	2.9738	1.14826	59.476	Moderate
I have a fear of being targeted for killing because of incitement and participation in campaigns in support of Gaza	3.0626	1.13916	61.252	Moderate
I have concerns about my family using my account to reach them and being blackmailed	2.9879	1.13701	59.758	Moderate
Total	3.074	1.1487	61.5	Moderate

It is clear from the previous table that the overall response to the axis of digital privacy concerns during October 7, 2023, war is moderate, at (61.5%) and in terms of the arithmetic mean (3.074).

The highest response was " I have concerns about the exploitation of my personal information and news from the Israeli side" at 63.2%, and the lowest response was " I have concerns about stealing my account and publishing what is not appropriate in it, as happened with many prisoners by publishing the phrase" I love Israel "at 59.4%.

The results of the qualitative study showed that digital privacy became more violated and weakened after the seventh of October because of systematic breaches by the occupation and the support of major technology companies in collecting data and converting them into individual personal files of Palestinians with the aim of prosecuting, arresting, or assassinating them.

The weakness of digital privacy after the seventh of October, in that the Israeli occupation revealed its qualifications and technological capabilities more than in the past, as the use of technology has become a means of following up social media platforms and punishing Palestinians, and many platforms that have provided technology with the occupation in an unprecedented way, such as Google, Amazon, and others, have resulted in the prosecution, arrest, and assassination of Palestinians, whether against the background of posting on social media networks, or against the background of users' conversations with artificial intelligence, or others. Many have been assassinated by tracking through the use of technology, and Israel has huge projects related to assembling millions of Palestinian conversations to collect them in a unified security system, and it has advanced and very modern systems that contribute to predicting behaviour by knowing the behaviour of users through their profiles through social media networks and applications based on their digital activity, which threatens their digital privacy and digital security, in addition to the camera technology and face tracking that have been used in a tremendous way in recent times.

The results of the study analysed the impact of social media policies on the activity of the Palestinian digital society after the seventh of October 2023, see Table 4.

Table 4

impact of social media policies on the activity of the Palestinian digital society after the seventh of October 2023

Item	Mean	Standard Deviation	Percentage (%)	Level
Social Media Policies Restrict Palestinian Content and Active Accounts	3.3745	1.13377	67.49	Moderate
Palestinian content on social media platforms was systematically deleted and restricted after 7 October	2.8707	1.12546	57.414	Moderate
Digital restrictions negatively affect the interaction of Palestinian society with political events	3.1313	1.10250	62.626	Moderate
Electronic monitoring of Palestinian content has led to caution in the nature of my digital activity	3.1230	1.14548	62.46	Moderate
Weak interaction with news about Gaza over time in digital platforms	3.0927	1.12612	61.854	Moderate
Many of the active pages supporting Gaza were closed during the war on Gaza due to the policy of digital platforms	2.9231	1.10418	58.462	Moderate
Total	3.085	1.1229	61.7	Moderate

It is clear from the previous table that the overall response to the axis of the impact of social media policies on the activity of the Palestinian digital society after the seventh

of October 2023 came with an average score of 61.7% and an arithmetic average of 3.085.

The highest response was "policies of social media platforms restrict Palestinian content and accounts active in it" at 67.4%, while the lowest response was "Palestinian content on social media platforms was systematically deleted and restricted after 7 October" at 57.4%.

The results of the qualitative study also showed that there is a restriction by technology companies of Palestinian content, in which content that supports the Palestinian cause is often deleted and pursued, and most respondents confirmed this.

Discussion

The results of the study revealed that Palestinian users of digital platforms have an average awareness of digital privacy at 60.7%, and this awareness was reflected in the nature of their perceptions towards digital security, which reached 60.4%, and their concerns related to digital privacy at an approximate rate of 61.5%, which prompted them to take measures and ways to protect against digital violations on an average of 61.6%. The impact of social media policies on their activity is average at 61.7%, and this is evidenced by the policies of restriction and prohibition of Palestinian content, and therefore the level of political participation is also average, which explains the average direct relationship between digital privacy, digital security and digital political participation in Palestinian society during the war on Gaza.

The level of awareness of users of digital platforms, and their medium awareness of digital privacy is the main reason for the emergence of fully medium results, because this awareness formed medium perceptions and concerns about digital security, and therefore their activity was within this average, and if they had greater awareness, the concerns would have been greater, and this was translated either by using higher protection methods and better political participation, or by total distance and less political participation, as evidenced by the theory of telecommunications privacy management, which emphasizes that the individual's motivation to protect against risks and threats stems from perceived severity, weakness and effectiveness of the response (sedek, 2018)

The results showed that users of digital platforms were aware of the perceived severity and risks to a moderate degree, as well as the perceived vulnerability, including the possibility of being arrested, stalked, or killed, but with a medium probability, which affected their levels of political participation in a moderate way. Thus, the level of medium awareness in digital privacy affected levels of anxiety, and this was reflected in medium privacy protection behaviours.

Concern about information privacy has had an impact on privacy protection behaviour strategies, and within the framework of communications privacy management theory, concern about information privacy is an intermediate variable that explains the relationship between the factors involved and privacy protection behaviour strategies (Stern, 2017).

In the same context, awareness of digital privacy is reflected to an average degree on people's stress levels. According to the theory of communication privacy management (Petronio, 2023), this will be reflected either by refraining from digital political participation and reducing the use of social networking sites, or by providing digital protection methods. However, in this study, medium awareness and tension affected the use of medium protection methods and medium levels of policy participation as well, i.e. partial reluctance in line with the levels of fear, anxiety and tension from digital risks, threats and violations.

The results also showed that the methods of protection used are medium and varied as well. According to the theory of privacy management, users' decisions to disclose, anonymize, or follow strong protection measures explain how they manage their political and communication interaction in the insecure digital environment, and formulate digital political participation considering the threats they are exposed to during the recent war on Gaza. This was confirmed in the theoretical framework of the study that individuals have a motivation to rely on protection behaviour to adapt and adopt behaviours to control risks and threats. Adaptation strategies can be divided into two dimensions, namely: proximity and avoidance strategies include falsifying personal information and seeking social support, while avoidance strategies include withholding personal information (Chen, 2017).

This applies considering the theory of communication privacy management, through which there is a direct relationship between privacy and digital security for political participation through social digital platforms. This involves the Palestinian environment, as digital violations in Palestine, especially considering the war on Gaza, have prompted many to adopt adaptation strategies that seek to alleviate pressures or their sources.

The results of the qualitative study also showed that Palestinian users of digital platforms suffer from varying levels of awareness of digital privacy and digital security, but they are fully aware of the nature of the risks they may face from arrest, prosecution, killing, or even extortion, which are images translated daily during the war on Gaza, clearly and publicly.

The level of privacy awareness in Palestinian society is medium, and this was evident in a study (Abu Arqoub, 2021) that agreed with this study in affirming that the concept of privacy and personal data is not known to most groups in Palestinian society, and that there is a need for intensive efforts to introduce it and its importance, and the reality of digital privacy is very weak because of this, in addition to the occupation practices that focus on penetrating Palestinian data in order to prosecute them.

On the other hand, the results confirmed that the weak reality of digital privacy, which eliminates digital security, creates fears of political participation. The results of the qualitative study showed that penetrations occur significantly to smart devices, taking advantage of people's use of them, to form a tool for hunting people in Gaza and monitoring them easily. Abu Adl also explained that after recent events and with the increasing use of digital space for expression and political participation, users, especially activists, have become more vulnerable to tracking information, deleting

content, and closing accounts, and this has reduced digital political participation clearly and explicitly.

This is in line with the results of a study (Graff, 2023) that confirmed the escalation of digital threats and violations during the war on Gaza. However, it did not address the levels of digital political participation directly, but it clarified how social media sites restrict Palestinian content, which may affect the nature of the results on the levels of digital political participation. Israel has pushed millions to ban Palestinian content to show that there is no effective political participation, which affects public opinion, and citizens to increase their fears of digital political participation at a time when it appears that everyone has stopped it, which is not true. The results of the quantitative and qualitative study did not deny the existence of digital political participation, but it took different forms and methods to protect and achieve maximum digital security.

The results of the study revealed that the level of awareness of digital privacy among citizens in Palestinian society is medium, and this was represented in their medium awareness of the concept of digital privacy, their prior knowledge of it, their medium awareness of the importance of preserving their personal data in digital platforms and the risks of disclosing it, and knowledge of the methods available to protect their digital accounts, as well as their medium knowledge of the laws and legislation that protect their digital privacy, but they are also aware that awareness of digital privacy is very important during the war on Gaza, and all percentages ranged from 57% to 61%.

This medium awareness of digital privacy was also translated to their medium awareness of privacy policies before using them, and their medium keenness towards unclear information, such as fake links and additions and anonymous or ambiguous messages. This medium awareness of digital privacy was reflected (Sulaimani, 2023) in the nature of their fears about it, which was confirmed by the fact that the Israeli occupation policy formed many fears among Palestinian youth for fear of their lives, or the lives of their loved ones, and some retreated from publishing pro-Gaza content for fear of arrest or killing, or being subjected to account theft and the subsequent process of blackmail or dropping, especially in light of the Palestinian party's conviction of the technological superiority of the Israeli side, in addition to the weakness of the privacy policy of social media sites, and its standing alongside Israeli content in most cases.

These results are consistent with a study (Ndlovu, 2023) that stressed the importance of knowing the basics of privacy, its rules and how to deal with them, especially during wars to prevent attacks and security prosecutions.

In addition, the results confirmed that the perceptions of Palestinian users of digital platforms towards digital privacy deepened after the 7th of October. They are aware that the use of digital platforms considering the war is unsafe, and that the war has increased digital and security risks, because a large part of the digital information of Palestinians is vulnerable to Israeli access. In addition, Israeli surveillance, tracking, and spying on personal data technologies have also motivated Israel to hack Palestinian accounts without pretexts. Therefore, digital security is subject to repression and threat

from several parties. In addition, privacy laws in cyberspace are insufficient to protect and prevent account theft. In addition, digital culture is insufficient to protect.

These results are consistent with the study of (Rizk & Cordey, 2023), which stressed the importance of knowing the control of digital information as it represents another battlefield that can affect the field war data.

Palestinians believe that the war was an excuse to deepen the impact of digital Israeli violations, with the aim of fighting Palestinian content and prosecuting its publishers. However, their knowledge of methods of violation, tracking and espionage is limited, but they are already aware of the risks and know that they are being monitored and that they will be held accountable for any content that encourages resistance.

This explains that their perceptions of digital privacy are medium, but their awareness of the dangers in light of the war is almost high, but their awareness of how to track and spy and how to protect is medium, and they know full well that the war has increased the digital Israeli violations that existed in the first place, but it has taken more expansive and accurate forms and methods than before, as indicated by (Human Rights Watch, 2024), which emphasized the Palestinian digital environment as a confrontation arena parallel to the field war, in which Israel uses artificial intelligence tools, espionage systems, and content restrictions to undermine Palestinian collective awareness and control the flow of information.

Rizk & Cordey 2023 also stressed that the humanitarian response has not yet understood the magnitude of digital risks to civilians in conflict, pointing to three types of digital risks in times of conflict, including those related to humanitarian actors to support humanitarian and protection activities, including those related to the use of armed actors to support military operations such as information and cyber operations against civilians, infrastructures, or the misuse of personal and humanitarian data, including those related to the reuse or dual use of technologies and infrastructure, and allows the involvement of civilians in conflict-related actions, such as surveillance, intelligence gathering or cyber and information operations.

The study believes that young people, with varying awareness, tend to take risks and venture, especially if they have faith in the justice of their cause, which has been confirmed by previous studies that faith in the cause leads to adventure. Palestinian youth have full faith in the Palestinian cause and love of sacrifice, but their weak awareness of digital privacy exposes them to these risks, and thus their participation has become medium.

This can be explained in the light of the theory of communication privacy management, in that the aspect of their awareness of perceived intensity is equal to their awareness of benefit or efficiency, and therefore this is reflected in their average perceptions towards digital security, in light of the war on Gaza, where the perceived intensity is the risk of losing the privacy of information on social media sites, which motivates them to adopt privacy protection strategies on social media sites.

A study showed (Ndlovu, 2023) that privacy concerns are related to tracking when browsing the Internet, where many find that targeted ads are intrusive, in addition to theft, where identity theft is a serious problem that is fairly widespread online, and

cybercriminals infiltrate accounts, computers, and phones using viruses, spyware, and phishing methods to obtain private information to be used in identity theft; As a result, sensitive information is likely to leak and lose vital data.

In any case, digital security in Palestine is a complex issue, and this is consistent with a study that showed (The Arab Center for Social Media Advancement, 2024)that the issue of digital security in the Palestinian context has become complex and complex as a result of the multiplicity of parties that violate Palestinian digital rights, and the diversity of sources of digital threats. It found that the Israeli occupation, digital platforms, and official Palestinian entities, along with individuals and private commercial companies, all violate digital rights and pose a threat, and its results reflected a significant gap in awareness and knowledge of digital security issues and practices for users, which makes them vulnerable to various digital attacks and threats.

The study explains the nature of the average awareness of digital security issues and practices among users of digital platforms in that they tend to ignore digital privacy settings, or not understand them, especially those in English, or that they tend to venture into displaying their own content, without ascertaining the correct foundations of protection, in addition to the fact that some of them resort to fake accounts that obviate the idea of learning digital privacy with its complexities and how to protect against espionage and follow up, and therefore these perceptions vary from one individual to another according to the degree of interest in digital privacy, and the nature of the content they share.

Conclusion

The results of the study revealed that the level of awareness of digital privacy among citizens in Palestinian society is medium by(60.7%), as their level of awareness and knowledge of digital privacy and its importance is medium, as well as the laws and legislation that protect their privacy, their awareness of the importance of preserving personal data and the risks of disclosing it is medium, and their knowledge of the methods available to protect their digital accounts is medium, and this was reflected in their average keenness towards ambiguous information such as fake links, or their average knowledge of digital privacy policies.

The study also concluded that the perceptions of users of digital platforms in the Palestinian society about digital security in light of the war on Gaza are average by (60.4%), as they consider that the use of digital platforms in light of the war is unsafe, as it has caused an increase in security and digital risks, and formed a motive for Israel to increase the violation of digital privacy, for espionage and surveillance, and they are aware that the laws are insufficient to protect them, as well as for digital culture.

The study found that the level of impact of social networking policies on the activity of the Palestinian digital society after October 7, 2023, came with a moderate degree of 61.7%. The result reveals the role of this impact in restricting Palestinian content on social networking sites and its exposure to deletion, and this reflects moderately on the interaction of Palestinian society with political events, as well as caution against digital political participation due to electronic surveillance, poor interaction with news

related to Gaza, and the closure of many pages supporting it, all of which range from 57% to 67%.

References

- Abu Arqoub, O. (2021). The reality of privacy and digital data protection in Palestine: an exploratory study. *The Arab Centre for Social Media Advancement- Tamleh, Palestine*.
- Adway, Abdallah, (2023) Israeli Propaganda: Reading in the Soft Power (2023). Istanbul: Vision Centre for Political Development.
- Al-Sharif, N. Y. (2022). Legal mechanisms dedicated to protecting the right to digital privacy in Algerian legislation. *Journal of Research in Contracts and Business Law*, 7(2), 192-213.
- Al-Masaeed, A. (2025). Privacy in the Digital Age between Theory and Practice considering International Standards: The Palestinian Context as a Case Study. *Published doctoral dissertation, Arab American University, Palestine*, 1-224.
- Al Jazeera (2021): The backbone of global espionage technologies... What do you know about Israel's Unit 8200? Retrieved 2-4-2024. See: <https://www.aljazeera.net/tech>
- Al Sayed, M. I. A. & Sayed, W.S. A. (2022) Values of Enhancing Digital Security among University Students in Egypt to Face the Challenges of the Digital Revolution. *Fayoum University Journal of Educational and Psychological Sciences*, 16(5), 340-427.
- Awad, A. F. A. (2021) Protect the digital medical file between privacy and information security. *Journal of Legal Studies and Researches*, Vol. 6, no. 1, pp.160-178.
- Husary, N. (2025). The Freedom of Digital Narrative for the Palestinian User. *Journal of Association of Arab Universities for Research in Higher Education*, 45(3), 63-81.
- Ibn Amra, B. (2024). Digital Transformation and Its Impact on Individual Privacy: The Question of Boundaries and Socio-Legal Frameworks. *Journal of Humanities*, 35(3), 271-285.
- Chen, H. B. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviours. *Computers in Human Behaviour*, 70, 291-302.
- Council of Europe. (2004). *Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (ETS No. 108)*. Strasbourg: Council of Europe. Retrieved from <https://www.coe.int/en/web/data-protection/convention108>
- Graff, A.-R. (2023). Covert Wars: Social Media and War Management in Gaza, Platform X in the Eye of the Storm: The Price of Truth. *Gulf Research Centre*. Retrieved from <https://www.grc.net/documents/656339d00c2efinvisibleWar2.pdf>
- Moussaoui, A. (2022). The Right to Privacy in the Digital Media Context. *Journal of Legal and Economic Studies*, 5(1), 1242-1278.
- Ndlovu, S. (2023). *The war on privacy: how to fight back with digital safety*. Retrieved from <https://en.hive-mind.community/blog/438,the-war-on-privacy-how-to-fight-back-with-digital-safety>
- Petronio, S. (2023). Communication Privacy Management Theory: Managing boundaries in digital contexts. *Journal of Communication Theory and Research*, 12(1), 15-32.
- sedek, M. A. (2018). Motivational factors in privacy protection behaviour model for social networking. *MATEC Web of Conferences* 150, 05014. (Vol. 150, p. 05014). EDP Sciences.

- Shaalal, M. a. (2022). Digital Privacy of Social Media Users: Between Protection and Violation. *Al-Mi'yar Journal*, 12(2), 1086-1095.
- Stern, T. &. (2017). Examining privacy settings on online social networks: a protection motivation perspective. *International Journal of Electronic Business*, 13(2), 244-272.
- Sulaimani, J. (2023). The digital privacy of the individual and the extent of the impact of cybercrime on it. *Journal of Law and Political Science*, 9(2), 88-98.
- The Arab Centre for Social Media Advancement. (2024). *Palestinian Digital Rights, Genocide, and the Responsibility of Big Tech Companies. Campaign*. Retrieved from The Arab Centre for Social Media Advancement.
- Buchan, R. (2023) *The Rights to Privacy and Data Protection in Times of Armed Conflict*. look: <https://ccdcoc.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf>
- Dahmani, S. & Jaraya, S. (2022). Digital Privacy During Crises: Reality and Challenges: The Coronavirus Crisis as a Case Study. *International Journal of Legal and Political Research*, 6(1), 107-125.
- Faqiha, B. (2022) Online privacy challenges and their forensic solutions. *Journal of the Arab American University*, Vol. 8, no. 1, pp.1-14.
- Human Rights Watch. (2024 September 10). *Gaza: Israeli Military's Digital Tools Risk Civilian Harm-New Technologies Raise Grave Laws-of-War, Privacy, Personal Data Concerns*. Hrw org site. <https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm>
- Ifex. (2025 January 29). *The War on Gaza: Digital rights violations and weaponization of AI*. Arab Centre for the Advancement of Social Media.
- Khadam, U. & Iqbal, M. M. & Alruily, M. & Al Ghamdi, M. A. & Ramzan, M. & Almotiri, S. H (2020) Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions. *Wireless Communications and Mobile Computing*, Vol. 2020, no. 2020, pp.1-15.
- Masoudi, M. (2022) Samples in descriptive research, *Researcher's Journal for Mathematical and Social Sciences*, 4(2): 247-263.
- Mahajer, M. & Nouari, A. (2022) Building a virtual identity and dealing with information privacy issues in light of social media network policies: Facebook users as a model. *Digital Journal for Media and Communication Studies*, 2(3), 156-170.
- Quds Network. (2020). What does it mean to download the Israeli "Coordinator" app on your mobile phone? Quds Net News Website. <https://qudsnet.com/post/488499>
- Rajab, S. A. M. & Najib, W. S. & Abd al-Maqsud, H. N. (2023) Awareness of digital privacy among users of new media. *Journal of Research in the fields of Specific Education*, Vol. 9, no.44, pp. 2495-2522.
- Rizk, J. & Cordey, S. (2023) What we don't understand about digital risks in armed conflict and what to do about it, *Humantary Journal*, Look: <https://blogs.icrc.org/law-and-policy/2023/07/27/digital-risks-in-armed-conflict/>
- xu, Z. & Luo, M & Kumar, N & Vijayakumar, P. & Li, L. (2020) Privacy-Protection Scheme Based on Sanitizable Signature for Smart Mobile Medical Scenarios. *Wireless Communications and Mobile Computing*, Vol. 2020, no. 2020, pp.1-10.

Othman, M. (2025). Freedom of Expression in the Digital Age: An Analytical Study of Hate Speech, Privacy and Legal Liability before the European Court of Human Rights. *Journal of Jurisprudential and Legal Research*, 49(49), 4451-4506.