FACTSHEET ON THE STATUS OF PALESTINIAN DIGITAL RIGHTS FOR CIVIL SOCIETY ORGANIZATIONS AND CONSEQUENCES OF THE GENOCIDE

As part of its work in the field of public and digital diplomacy to expand global communication outreach in support of the Palestinian cause, MIFTAH conducted an assessment survey on the cognitive capabilities of civil society organizations (CSO) in the West Bank, including Jerusalem and the Gaza Strip, on digital rights and its implementation.

This survey reflects the complex reality of digital rights in occupied Palestine and assesses how prepared CSOs are in dealing with growing digital challenges, especially after the 2023 genocide. The survey sheds light on the gaps in digital knowledge and the infrastructure for digital security, which is a particular challenge, hampering the ability of institutions to protect their data and effectively carry out their role.

The survey is based on the descriptive methodology, including questionnaires from 55 institutions in the West Bank (including Jerusalem) and the Gaza Strip, in addition to in-depth interviews with six digital rights, women's and other institutions working in the Gaza Strip. The qualitative data was analyzed using advanced tools such as Nvivo and SPSS.

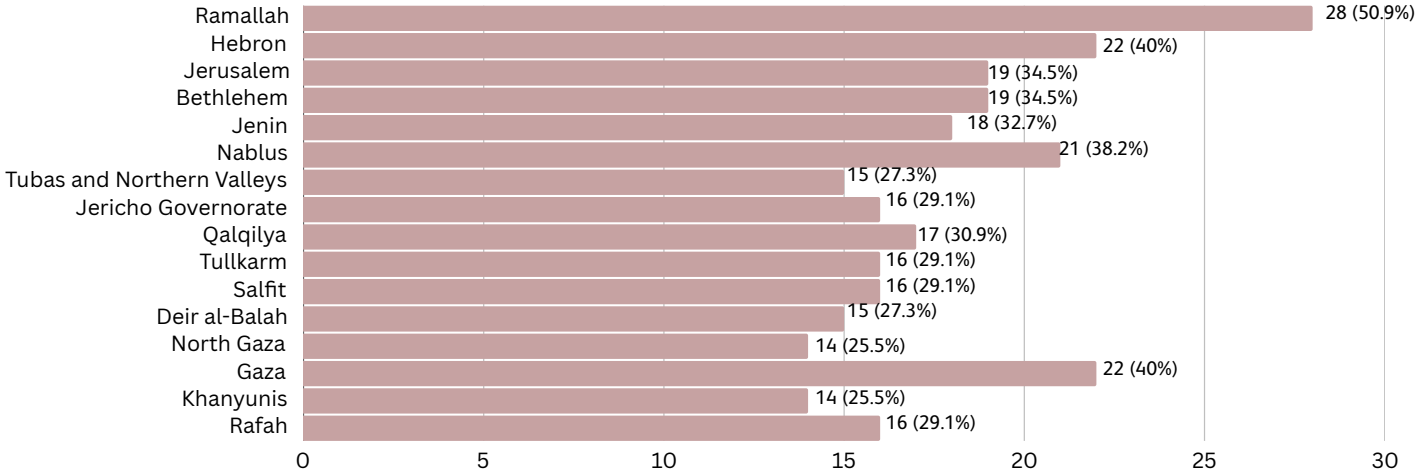
Overview

According to the outcomes of the survey, CSOs target various sectors, with women being the most targeted sector at 43.6%, followed by children, at 16.4%, the elderly at 12.7% and youth at 10.9%. Meanwhile, persons with disabilities were targeted at 9.1% and media persons at 7.3%. Furthermore, the results of the survey showed that 34.5% of CSOs target all sectors indiscriminately, thus reflecting the comprehensiveness of the sample.

The scope of the work of Palestinian institutions is distributed within the districts as follows: Ramallah, at 50.9% of institutions, Hebron, at 40%, Jerusalem at 34.5% and Nablus at 38.2%. It also extends to the Bethlehem, Jenin, Tulkarm and Salfeet governorates at 29.1% each and the northern Jordan Valley at 32.7%, Jericho and the Jordan Valley at 27.3% and Qalqilya at 25.5%.

In the Gaza Strip, the work of CSOs in northern Gaza stood at 40%, Khan Younis at 29.1% Gaza City at 40%, Rafah at 25.5% and Deir Al Balah at 27.3%.

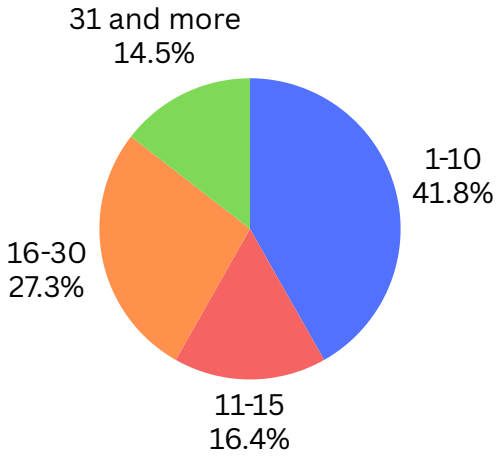
Graph: Distribution of CSOs in the various Palestinian districts



The locations of Palestinian CSO included in the survey were distributed among cities, camps and villages, with the majority of CSOs concentrated in cities, at 74.5%. Villages were the headquarters of 16.4% of the institutions while only 9.1% were based on camps. This distribution reflects the urban concentration of CSOs and highlights the need for increased presence in rural areas and in camps, to promote inclusiveness and access to marginalized and vulnerable sectors.

The size of Palestinian CSOs participating in this survey varied in terms of the number of employees. The survey showed that 27.3% of institutions include from one to 10 employees, while 16.4% have 11 to 15 employees. The largest majority of CSOs, 41.8% had between 16 and 30 employees while only 14.5% of institutions had over 31 employees. This distribution reflects the variety in size of CSOs, with most institutions either small or medium size, which is compatible with the survey sample.

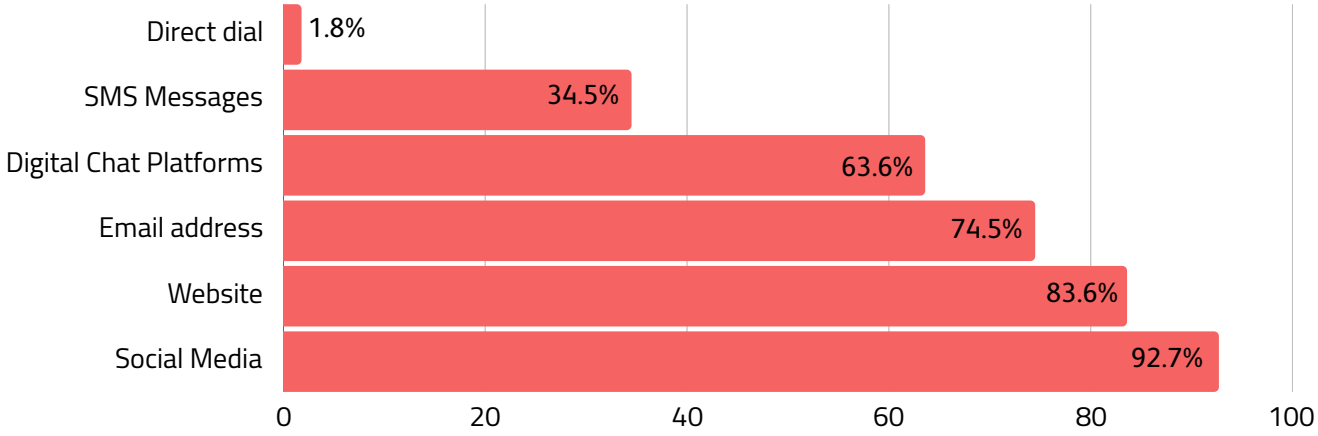
Graph 2: size of CSOs according to number of employees



Means of communication among CSOs

The CSOs depend on a variety of digital methods to communicate with the public and beneficiaries, with social media being the most common method used, at 92.7%. This indicates the significance of these platforms as the main channels for communication and dissemination, followed by websites, which are used by 83.6% of institutions. Another 74.4% of CSOs depend on email as a means of communication, while 63.6% use digital chat platforms such as Whatsapp. Even with the development of communications methods, 34.5% of CSOs still use SMS text messages, while only 1.8% depend on direct phone contact.

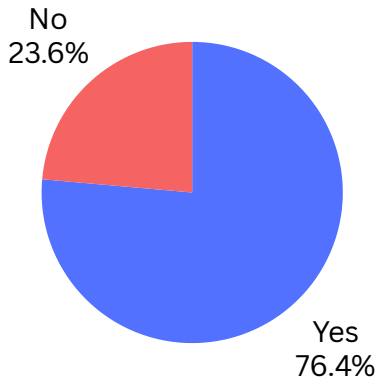
Graph 3: Digital methods used by institutions to communicate with the public and beneficiaries



Understanding and applying digital rights

The survey showed that 76.4% of institutions have knowledge on digital rights, while 23.6% lack this knowledge, which indicates there is a significant sector of institutions that need increased knowledge and understanding of these rights.

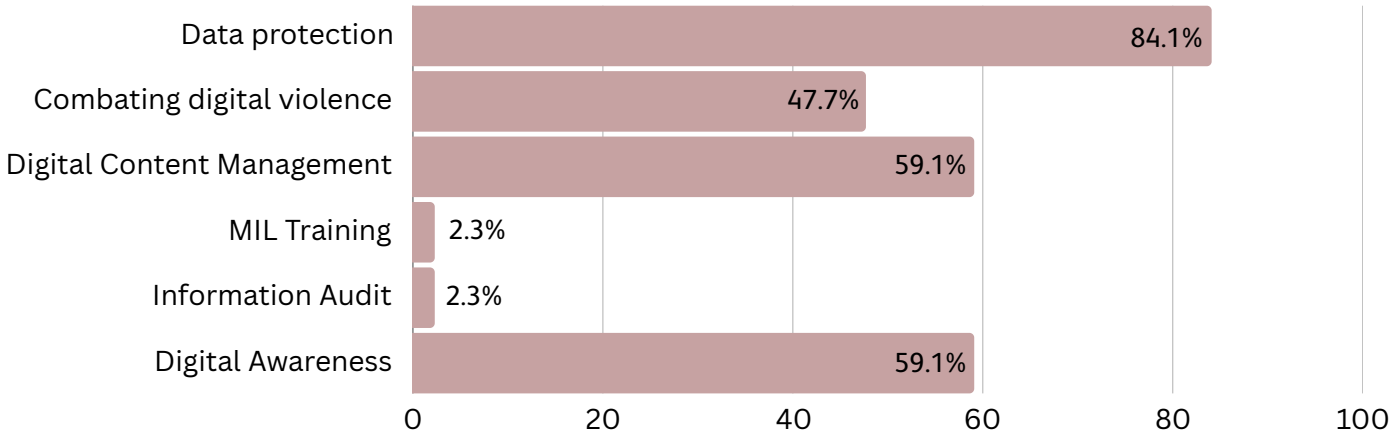
Graph 4: Knowledge of digital rights among institutions



The results show a clear relationship between the headquarters of institutions and their understanding of digital rights. According to the survey, in cities, 86.0% of institutions have a clear understanding of digital rights, while 14.0% lacked this understanding. In villages, institutions that had a clear understanding of digital rights stood at 66.7%, compared to 33.3% which lacked this understanding. In the camps, only 16.7% of institutions had a clear understanding of digital rights while 83.3% did not.

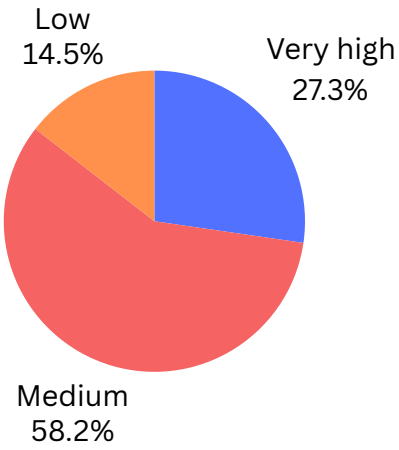
The institutions that said they had a clear understanding of digital rights and how to apply them in their everyday work, focused on several main points to boost this knowledge. The first point was protection of personal data, constituting a priority for 84.1% of these institutions. Combatting violence was considered a necessity, at 47.7%, while institutions also afforded considerable attention to managing digital content and digital awareness at 59.1%. Meanwhile, these institutions also pointed to the importance of the flow of information and media education, albeit at a lower rate. This focus reflects a growing awareness of the need for capacity-building in the fields of protection and content management in a way that guarantees the promotion of digital rights in a more effective and sustainable manner.

Graph 5: Digital rights focused on by CSOs



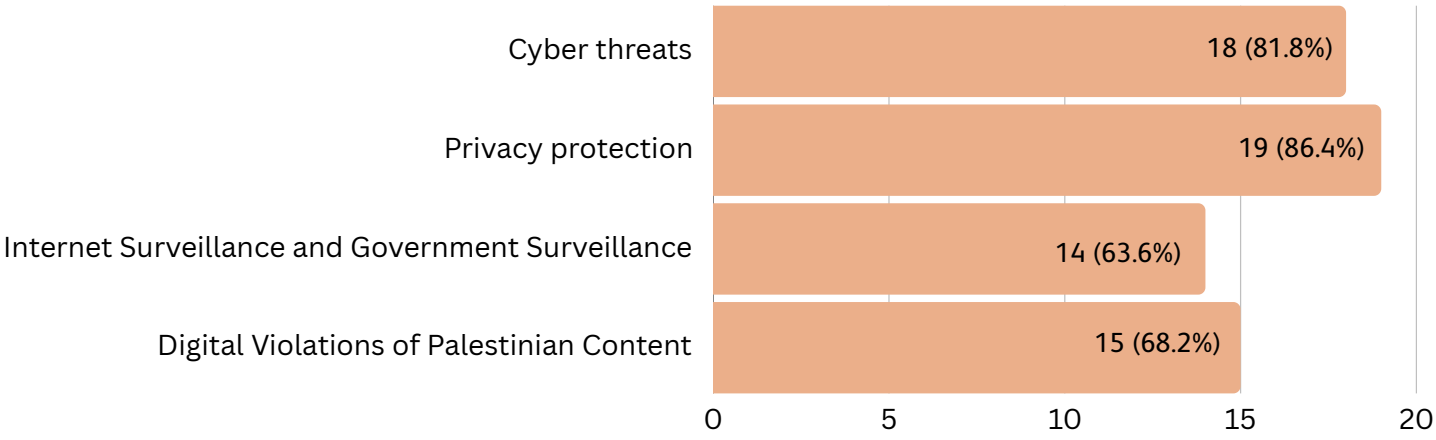
In regards to knowledge pertaining to digital threats and violations, the survey showed that 58.2% of institutions categorize their knowledge of digital risks as ‘moderate” while 27.3% said it was ‘low”. Furthermore, only 14.5% believed they had a ‘high level’ of knowledge on the subject. This illustrates the discrepancies in awareness levels among institutions and the need to increase knowledge around digital threats.

Chart 6: Digital rights focused on by CSOs



In regards to the institutions that categorized their understanding of digital rights as 'low' results showed the need to strengthen several areas: privacy protection was the number one area, with 86.4% of institutions expressing desire to improve their capabilities in this regard. Cyber threats came in second, at 81.8%, indicating a growing concern over digital security. Furthermore, 68.2% of institutions expressed their need for more knowledge regarding digital violations of Palestinian content, while 63.6% of institutions believe that internet and government monitoring needs more attention.

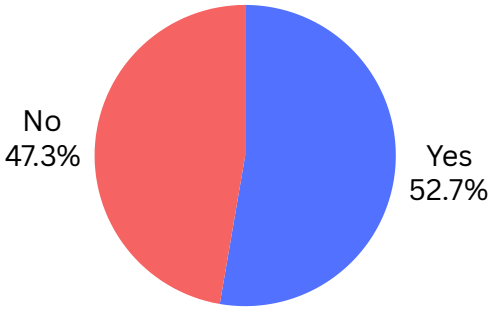
Chart 7: Enablement necessities to improve understanding of digital rights according to institutions



Policies of protection for digital rights

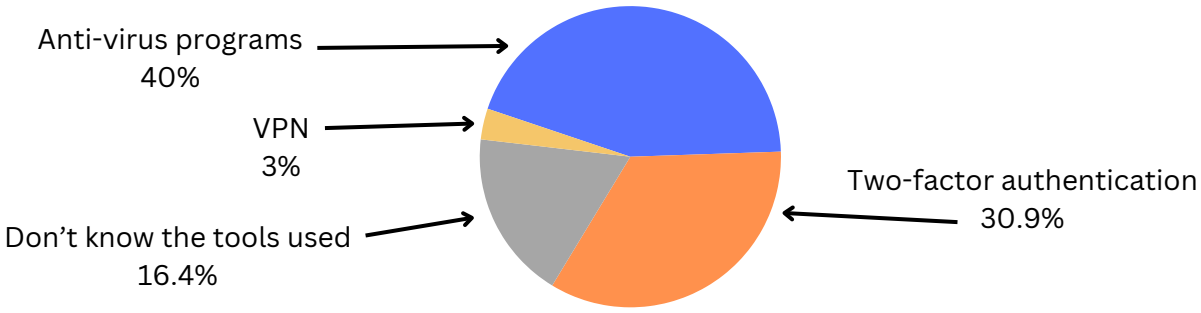
The survey results showed that 52.7% of institutions have no specific policies for protecting digital rights, while 47.3% have implemented policies such as privacy policies.

Graph 8: Percentage of institutions with digital rights policies



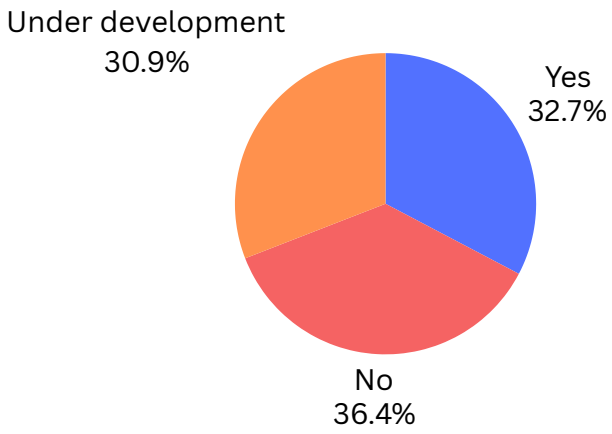
The data on digital tools, which institutions depend on to safeguard their information and data, showed that 40% of institutions use anti-virus programs as the main method of protection. Furthermore, 30.9% depend on two-factor authentication to enhance digital security while 16.4% of institutions indicated they do not use data-protection tools. This could reflect a lack of technical knowledge among some institutions. There is also a small percentage of institutions that depend on VPN (Virtual Private Network), encryption programs and other tools, but these were at a lower percentage than the other choices.

Graph 9: digital tools used to safeguard data and information in institutions



In regards to institutions adopting a clear policy on the personal digital data of women and girls, there were a variety of viewpoints from the respondents. 32.7% of institutions said they followed a clear policy in handling data, with around one-third of institutions who actually have a policy for protecting personal data. Meanwhile, 36.4% of institutions said they did not have a clear policy, while 30.9% of institutions said their policies were currently being developed but have not been implemented in full.

Graph 10: Extent of which clear policies for protecting the personal data of women and girls has been adopted

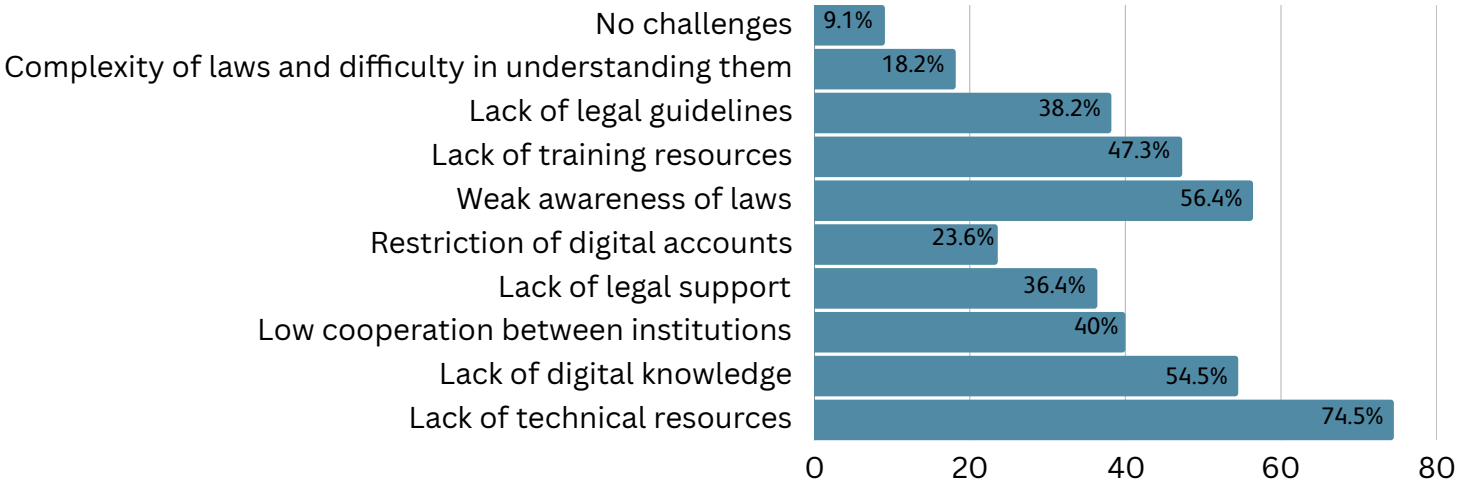


Challenges to protecting digital rights

74.5% of institutions stated they lack technical resources, while 54.5% said they lack digital knowledge and 40% of institutions said lack of cooperation between institutions was a major challenge. Another 36.4% said they lack legal support and 23.6% of institutions said their digital accounts have been restricted.

56.4% of institutions consider the lack of awareness around laws presents a major challenge, while 47.3% suffer from a lack of educational resources and 38.2% believe the absence of legal guidelines increases difficulties. Only 18.2% of institutions said laws were too complicated and difficult to understand while 9.1% said they did not face any mentionable challenges.

Graph 10: Main challenges facing institutions pertaining to digital protection

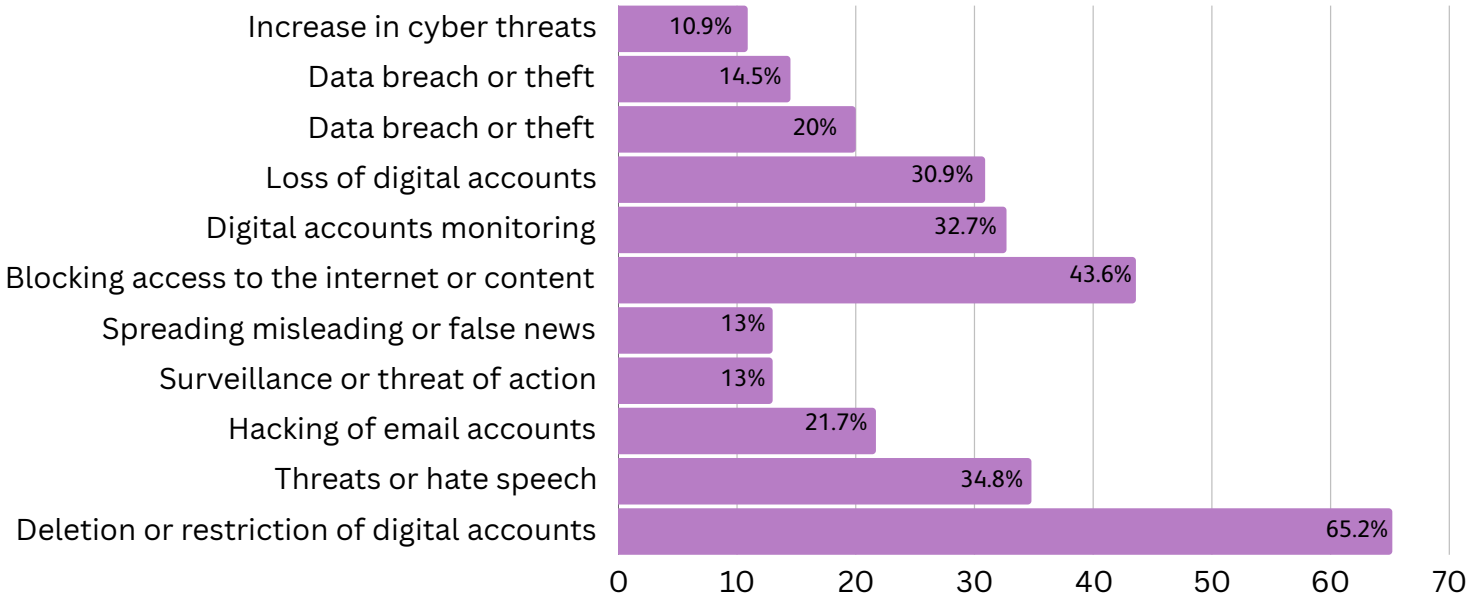


Digital rights during genocide

The survey showed that following October, 2023, 60% of institutions said they had not faced any direct digital violations, while 40% said they had directly experienced violations. As for the institutions that experienced violations, the most prominent of these violations was the removal or restriction on digital sites, at 65.2%, followed by online threats or hate speech, at 34.8%, then email hacking at 21.7% followed by other violations such as censorship or threats of action against digital content and the dissemination of misinformation, representing 13% each.

Furthermore, institutions faced other major digital challenges, including denied access to the internet or shadow-banning of digital content, at 43.6%, monitoring of digital accounts, at 32.7% and an increase in cyberattacks at 30.9%.Meanwhile, 20% of institutions said their digital accounts were shut down while 14.5% said their data had been hacked or stolen. Another 10.9% said cyber threats had increased against institutions.

Graph 11: Most prominent digital violations faced by institutions post October 7, 2023

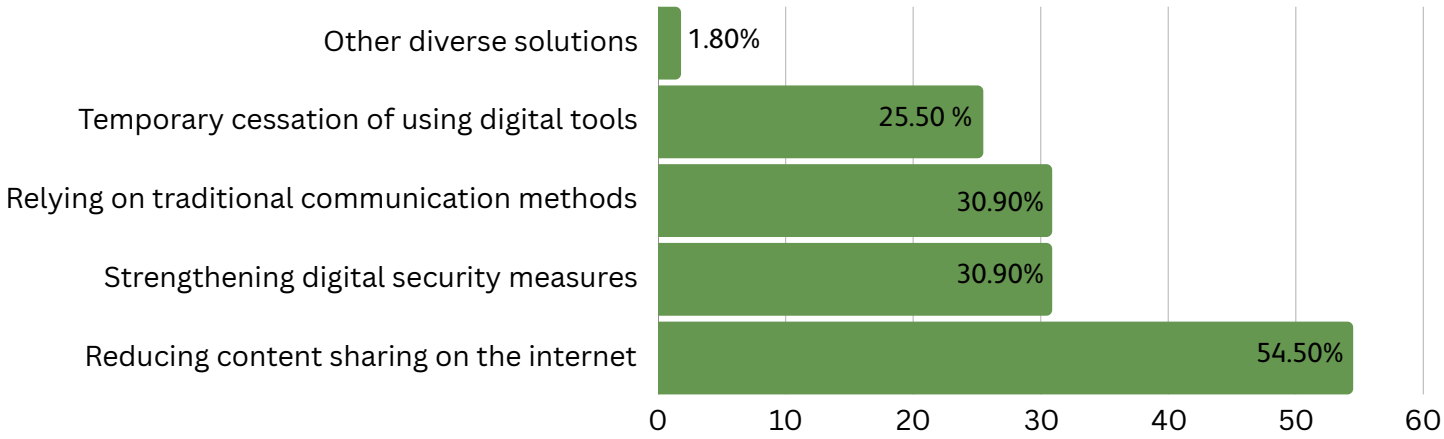


In regards to how institutions handled these digital threats and violations after October 7, 2023, 41.8% of institutions said they applied internal policies of protection against these threats, while 32.7% of institutions said submitting reports to the relevant parties was their main measure, while 25.5% of these institutions said they chose to cooperate with legal parties in handling these challenges. 16.4% said they offered psychological and technical support to the victims while 20% of institutions indicated that they did not directly deal with these threats or violations.

In regards to the impact of this escalation on the use of technology or on the documentation of violations and communication with beneficiaries, 54.5% of institutions said they were forced to decrease their digital content on the internet as a precautionary measure, while 30.9% of institutions said they had taken additional digital security measures while 30.9% said they depended on traditional communication means instead of digital ones.

Furthermore, 25.5% of institutions temporarily halted their use of digital tools, while a small group of institutions (1.8% for each) resorted to a variety of other solutions such as trying to beat the algorithm on social media sites when there is reduced engagement with posts.

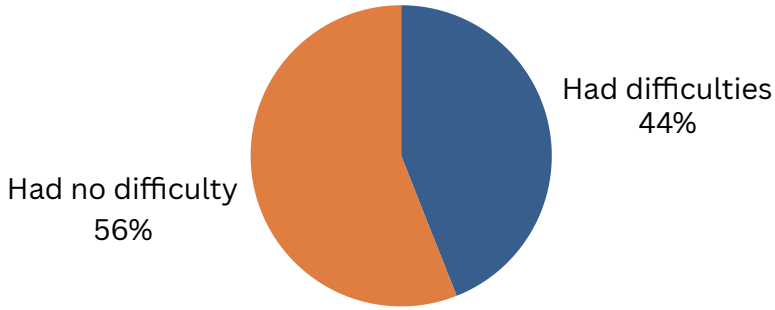
Graph 12: Most prominent variables in the use of technology and e-communication after October 7, 2024



Access to the internet as a digital challenge

The survey results showed that 56.4% of institutions had no difficulties in accessing the internet or other means of communication during the events while 43.6% said they faced major difficulties that affected their performance. These difficulties included repeated interruptions in internet services and electricity shortages, which led to a temporary halt in their work or delays in communicating with beneficiaries and colleagues, especially in areas most affected such as the Gaza Strip and Jenin. The participants stated that these cuts had a huge impact on the ability of institutions to document events and look into information after the destruction of the communications infrastructure resulted in difficulties of movement and contact between employees.

Graph 13: The scope of difficulties faced by institutions in accessing the internet



In addition to logistical difficulties, some institutions said attempts to hack their websites had been made and that there was increasing pressure due to content monitoring and posting restrictions, which increased the challenges to carrying out their duties efficiently. Furthermore, internet outages for long periods due to bombardment and repeated displacement prevented establishing any temporary, alternative means of communication, resulting in the isolation of some field teams who had no means of accessing alternative communication lines. In these circumstances, some institutions were forced to travel on foot to reach beneficiaries. This shows the serious challenges institutions face in continuing their fieldwork and efficiently providing services in an extremely complicated and tense atmosphere.

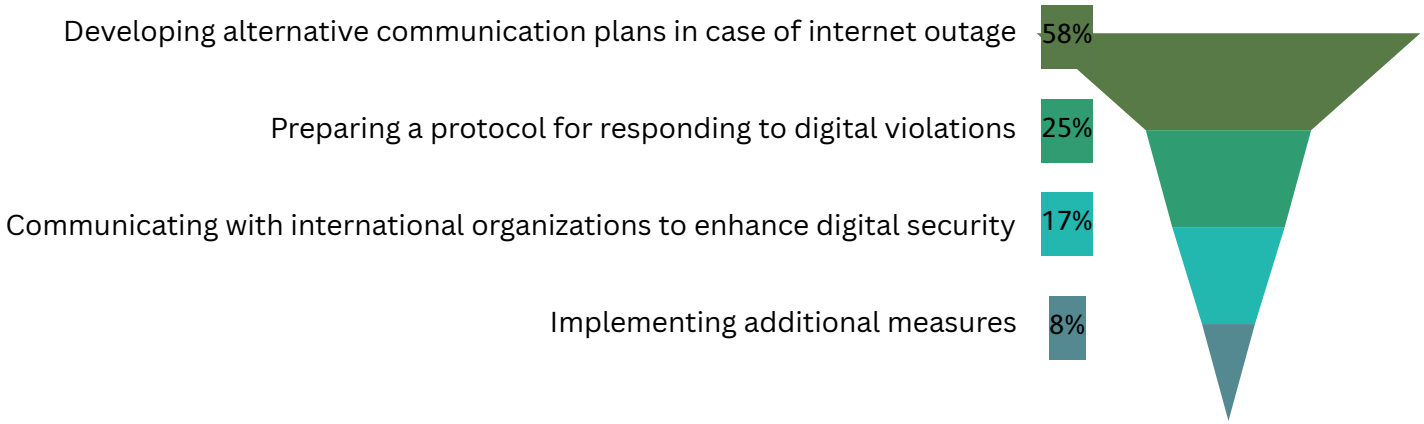
According to the results, institutions took several measures to reinforce digital security after October 7, 2023, the most prevalent being activating the two-factor authentication for all accounts. 50.9% of institutions adopted this method, followed by a review of privacy policies and data protection, at around 33%, which reflects the importance of protecting sensitive information. Furthermore around 26% of institutions trained employees on how to deal with digital threats and cooperate with other rights organizations to strengthen protection. Another 16.4% of institutions indicated they had not taken any specific measures, while 9.1% said they did not know about the measures taken. Among the less prevalent measures, 1.8% of institutions said they had activated the two-factor authentication of most accounts or are working on creating new websites as an additional procedure. These results illustrate the institutions' awareness of the importance of digital security and their approach towards reinforcing protection in the face of growing threats.

Graph 14: measures taken by institutions to strengthen digital security after October 2023

Digital emergency response plan

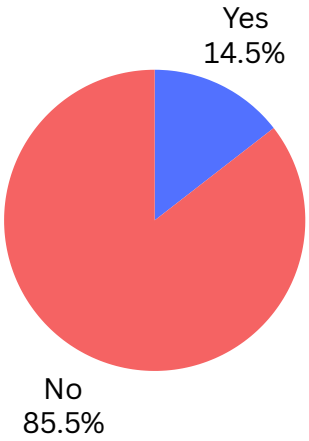
The survey results showed that 80% of institutions did not develop a digital emergency response plan after the latest escalation, while only 20% did. In regards to the institutions, which did develop a plan, their procedures varied within their respective plans. 58.3% said they formulated alternative communication plans if the internet was cut, while 25% said they prepared a response protocol for handling digital violations. 16.7% of institutions said they communicated with international parties that support digital security. Finally 8,3% said they prepared additional measures as part of their response plan. These steps illustrate the importance of formulating digital emergency plans, even though the majority of institutions have not yet taken this step.

Graph 15: Most significant measures taken by institutions that developed an emergency digital response plan



The survey result showed that the overwhelming majority of institutions, or 85.5%, did not receive any technical or legal support in confronting digital threats after October 7, 2023. Meanwhile, 14.5% of institutions said they had received support in facing these challenges. These results point to a major gap in the support available to institutions in confronting digital threats, which could increase interest in developing effective support networks in this regard.

Graph 16: Breakdown of institutions that received technical or legal support to confront digital threats after October 7



58.2% of institutions said they noticed an increase in digital solidarity from international and local parties following violations against them. This solidarity varied between technical support, (36%), financial support to develop a digital infrastructure (16%) and media campaigns to spread awareness, (80%).

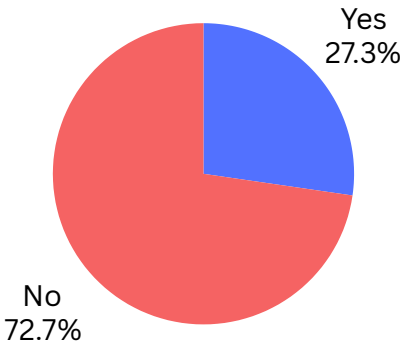
Documentation of digital violations

74.5% of institutions did not document digital violations, while 25.5% did. Among those which documented violations, 68.8% only conducted internal documentation while 31.3% cooperated with other rights organizations. 56% of the institutions faced restrictions or difficulties in documenting violations, including censorship of posts (65.2%) and direct threats of activists (65.2%)

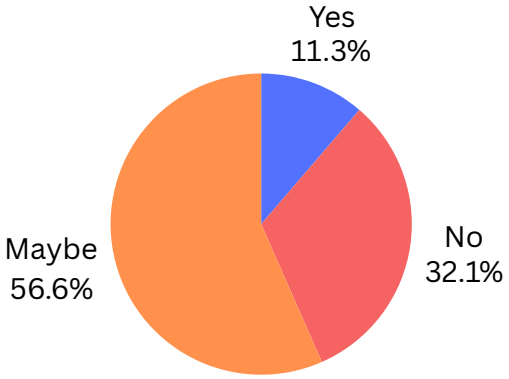
Palestinian legislation for protecting digital rights

The results show that the majority, or 72.7% of CSOs that participated in the survey do not know about local legislations or policies pertaining to the protection of digital rights in the digital space, while only 27.3% said they did know about these laws. As for how effect the cybercrimes law is in protecting CSOs from digital violations, organizations were split in their opinions, with 56.6% that said they might be effective while 32.1% said they were ineffective and only 11.3% that said they were actually effective.

Graph 17: knowledge of local legislation and policies for protecting digital rights in the digital space



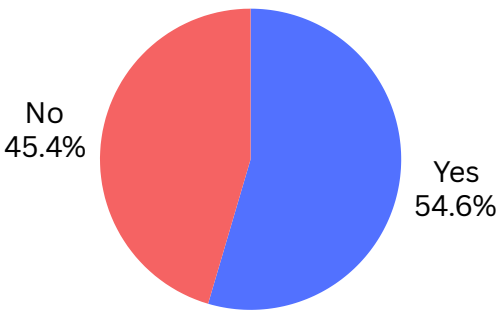
Graph 18: position on the cybercrimes law and protection of CSOs against violations



As for Palestinian government efforts to protect Palestinians from digital violations, 61.8% of institutions said the government was not making enough effort, while 7.3% said its efforts were enough and 30.9% did not know how effective the efforts have been. In regards to the mechanisms of filing complaints locally against digital rights violations, the results were close. 50.9% of institutions said they knew about the mechanisms for filing complaints while 49.1% said they did not know about them.

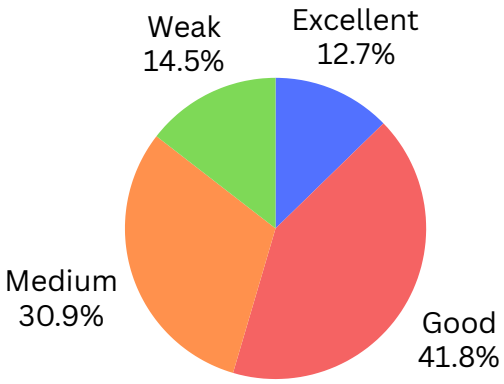
Regarding international laws, 54.4% of institutions said they had knowledge of certain international laws and agreements, which promote digital rights and support free access to the internet, while 45.5% said they did not know about these laws.

CHART 19: Breakdown of institutions with knowledge on international laws



Upon assessment of the level of knowledge of "free access to the internet" in international laws, 41.8% of institutions said they considered their knowledge to be weak, while 30.9% said they had medium-level knowledge, 14.5% who said their knowledge was good and only 12.7% who said it was excellent.

Chart 20: Level of knowledge among institutions pertaining to free access to the internet.



In regards to the importance of international laws and agreements local governments should abide by to ensure digital rights for the Palestinians, 88% of institutions said laws on freedom of opinion and expression were the most important, followed by data protection laws, at 76% and anti-digital discrimination laws at 52%, with laws guaranteeing free internet access coming in last, at 68%.

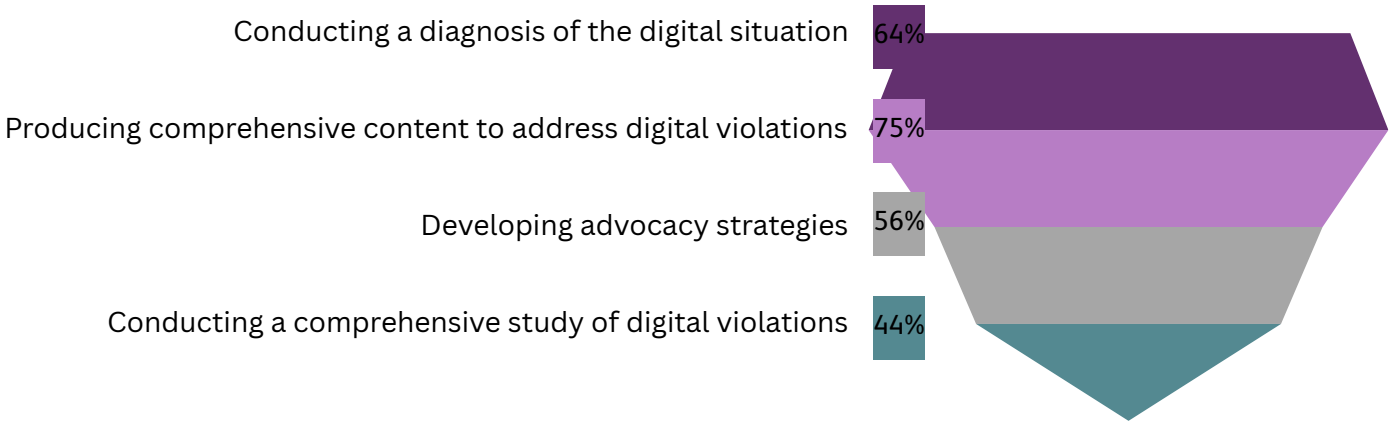
Institutional needs pertaining to protection of digital rights

67.3% of institutions said they wanted training on the fundamentals of digital rights, while 63.6% said they wanted training on national laws and 60% want training on international laws. Another 63.6% of institutions said they also wanted training on mechanisms to file complaints.

On digital security, 76.4% of institutions said they wanted training on this topic, while 72.7% said they needed tools of protection, such as anti-virus and encryption programs. 63.6% said they wanted to strengthen cooperation with international institutions, while 49.1% said they wanted to build joint support networks with other institutions. Only 16.4% said they did not need additional training.

63.6% of institutions suggested performing a digital-status diagnosis, while 74.5% recommended producing comprehensive content for handling digital violations. 56.4% said they suggested developing advocacy strategies and 43.6% said they recommended a comprehensive study of digital violations. This shows the need for a better situation analysis in this regard.

Graph 21: recommendations by institutions to promote digital rights protection



Most significant gaps indicated in the survey

Aspect	Points of weakness/gaps	Impact
Digital infrastructure	Lack of access to advanced technology such as 5G with dependence on outdated infrastructure like ADSL lines	Limits efficacy and hinders quick exchange of information
Digital awareness	Decrease in awareness of digital rights among 23.6% of institutions; acute shortage of training programs	Contributes to increasing vulnerability to digital threats and limits preemptive measures
Application of policies	Absence of comprehensive policies to protect digital rights in 52.7% of institutions	Puts institutions at risk of hacking and misuse of data
Availability of resources	Shortage of technical resources (74.5%) and legal support (36.4%)	Weakens ability of institutions to effectively respond to digital challenges
Digital security	Insufficient dependency on encryption and advanced security tools; limited awareness of cyber-threats	Increases risk of data violations and limits protection against advanced cyber-threats
Documentation and reporting	74.5% of institutions do not document digital violations; limited ability to cooperate in the field of reporting	Hampers efforts to hold violators accountable and to defend digital rights
International support	Dependency on short-term international funding; difficulties in establishing sustainable partnerships	Stymies long-term strategic planning and the ability for digital steadfastness
Digital monitoring	Repeated digital monitoring and targeting of content and platforms through calls by authorities	Creates an atmosphere of intimidation and self-censorship among institutions and individuals
Legal framework	Weak legislative framework; absence of comprehensive data protection law in Palestine	Fails to provide a trustworthy mechanism for protecting institutions and individuals