حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

# Digital Safety of Palestinian Children in East Jerusalem:

## Between Violations and Digital Agency

January 2025

7amleh - The Arab Center for the Advancement of Social Media
**January 2025**

# Digital Safety of Palestinian Children in East Jerusalem: Between Violations and Digital Agency

**Author:** Afnan Kanaaneh
**Design:** Majd Shurbaji
**Translated by:** DarLaila Publishing



Contact us:
Email: info@7amleh.org
Website: www.7amleh.org
Telephone: +972 (0) 7740 20670
Find us on social media: **7amleh**

## Table of Contents

# 1. Executive Summary

The discourse on human rights and children's digital rights is influenced by colonial contexts, power structures, and military and security operations. Within these contexts, international conventions often lose their validity and legitimacy due to the classification of children as a security threat to states,[1] present suspects, and "potential criminals" in the future, rather than as victims of ongoing military and political violence and aggression that target them and their childhood, or as a group that enjoys special moral protection. As a result of this classification, children become a fourth oppressed minority within developing countries that are persecuted and severely affected by war, thus, legitimizing a wide range of adult abuses.[2] This is the case in East Jerusalem, where Palestinian children are being dehumanized and stripped of their rights and the distinctiveness granted to children by international law.

This paper is intended to study the digital safety of Palestinian children in East Jerusalem, given that technologies are undergoing an accelerated process of integration into the societal infrastructure, thus, became an essential component in family life, work, profession, business, relationships, education, and governments,[3] and in all societal and cultural structures and frameworks in which children are involved. Particularly, the paper explores the level of awareness among children about digital risks, and their knowledge of digital protections. In addition, the paper examines the role of social actors (Israeli authorities, peers, families, schools, and civil society organizations) in undermining or promoting children's digital rights. The study is based on a vision that recognizes children as independent and present human beings and social actors, not merely as a "Potential future beings." Thus, the paper calls for focusing on children's opinions and experiences because of their underlying importance.[4]

1. Kovner, Bella. (2020). "Children's rights, protection and access to justice: The case of Palestinian children in East Jerusalem". In: Roer-Strier, Dorit; Nadan, Yochay. (Edited). Context-informed perspectives of child risk and protection in Israel: Pp. 241-261.
2. Feldman, Allen. (2002). "X–children and the militarisation of everyday life: comparative comments on the politics of youth, victimage and violence in transitional societies." International Journal of Social Welfare 11(4), pp. 286-299.
3. Third, Amanda; Livingstone, Sonia; Lansdown, Gerison. (2019). "Recognizing children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice." In: Wagner, Ben; Kettemann, C. Matthias; Vieth, Kilian. (Edited). *Research handbook on human rights and digital technology*. Edward Elgar Publishing. 376-410.
4. Lee, Nick. (2013). "The extensions of childhood: Technologies, children and independence." In: Hutchby, Ian; Moran-Ellis, Jo. *Children, Technology and Culture*. (Edited). London: Routledge. pp. 153-169

In its first section, the paper reviews the role of children's social environment in digital violations and attacks on them.
The second section reviews digital attacks on children based on a political background in the aftermath of the seventh of October, while distinguishing between the role played by the Israeli authorities and forces, and that played by technology companies.
In the third section, the paper reviews the role of caregivers in children's experiences and digital safety, including the role of parents and families, schools, and civil society institutions. In the fourth and concluding section, the paper reviews protection mechanisms, and tools common among children, and the social networks that children turn to for getting help and support when they are exposed to digital attacks.

The paper asserts that children's experiences and digital safety are shaped by a combination of gender, societal, economic, and political factors, in addition to factors related to educational relationship between the child-parent and school. Despite the impact of the mentioned factors, children are still able to rediscover their childhood by asserting their autonomy and digital and social activism, which turns them into targets of the regime's repressive policies.[5]

The paper concludes with a set of recommendations, the most important of which is the need for digital education for all caregivers of children, the need to enhance digital security within civil society institutions and schools, and the installation of digital safety for children as an additional and central perspective in civil society organization's work with children. In addition, the paper emphasizes the necessity to integrate digital security into educational curricula, protocols, policies and future plans for schools and institutions, and to work on developing interactive and entertaining trainings that convince children of the importance of digital security.

# 2. Literature Review

## 2.1 Who is a child? About the concept of childhood

In 1924, the Geneva Declaration of the Rights of the Child granted children recognition of their agency and activeness in society, while considering that they are still developing and must be granted special rights. In 1989, the United Nations Charter on the Rights of the Child replaced the Geneva Declaration, establishing a comprehensive legally binding framework of principles for the protection and promotion of children's civil, political, social, economic, and cultural rights. The Convention defines children as individuals under the age of eighteen, i.e., under the age of maturity under the law applicable to them.

5. Feldman, Allen. Ibid.

The Convention guarantees children special protection within the context of the family and society, including appropriate legal protection,[6] to ensure their mental and physical growth and development, and to enable them to participate socially and politically.[7]

In the introduction to the third edition of Readings in Indian Sociology: Sociology of Childhood and Youth, sociologist Bula Bhadra reviews the developments and transformations that have taken place over the years in defining, understanding, and conceptualizing the concept of childhood in sociological studies. Bhadra begins with a review of the socialization paradigm, which discusses how children are raised to become part of society. According to this model, children are passive recipients of values, norms, laws, and social conventions that adults instill in them. This socialization process aims to transform children from helpless and unqualified individuals into qualified adults who can contribute to society. This theory treats children as social property, focusing on what they might become in the future rather than considering them as human beings living in the present. This theory also ignores the fact that the role of children is not limited to absorbing societal norms but also interacting with these norms and reformulating them.[8]

Only with the beginning of the 1980s a more critical intellectual paradigm was developed, namely "the social structure of childhood", which considers children as independent individuals and social actors. This intellectual paradigm suggests that childhood is a developmental stage shared by all individuals under the age of eighteen. However, the nature and form of childhood is related to children's daily behaviors and the way they exercise their agency over their lives. Moreover, the social structure of childhood depends on a complex combination of intersecting factors, such as community structures, national and cultural contexts, individual practices and behaviors of children and adults alike, political, and economic institutions, laws, ethnicity, gender, and other factors within which a child is raised. Thus, this intellectual model believes that the formation of childhood is linked to external factors related to context and internal factors related to the child's agency, activism, and activeness.[9]

## 2.2 Techno-childhood

Children today are undergoing a technolization process.[10] They grow in an environment saturated with digital and cultural technologies,[11] as technology no longer plays a secondary, complementary, or recreational role only, but has become valuable and basic means through which to live their lives, and a tool that fulfils their needs in communication and

6. The United Nations. (ND). Convention on the Rights of the Child. Retrieved (19 December 2024) from: Click here.
7. Amnesty International. (ND). Children's rights. Retrieved (December 19, 2024) from: Click.
8. Bhadra, Bula. (Editor). (2013). Readings in Indian Sociology: Sociology of Childhood and Youth. California: SAGE Publications.
9. Ibid
10. Lee, Nick. Ibid.
11. Oswell, David. (2013). "Ethics and techno-childhood." In: Hutchby, Ian; Moran-Ellis, Jo. (Edited). *Children, Technology and Culture*. London: Routledge. Pp. 170-183.

acquisition of knowledge and information.[12] This development has called the studying of the relationship between childhood and technology, and the influence of technology on childhood, especially on its role in shaping, establishing and managing childhood. Nonetheless, children are active users of technology. Their use of technology is influenced by a wide and complex network of political, economic, and cultural factors that in turn contribute to shaping childhood.[13]

Therefore, there is a trend in the field of techno-childhood that simply considers technology as a mediator in many central phenomena in children's lives, i.e., a means of mediating between people, places, activities, and social interactions. In other words, while academic and social discourses tend to separate the digital sphere from reality, practices related to the use of technology in everyday life are still linked to the formation of traditional phenomena of childhood studies, such as: Identity, friendship, sharing, learning, family, place, play, deprivation, risks and more. Therefore, technology did not contribute to creating a radical break from childhood known in the past, but rather led to an evolutionary transformation in it, as children experience the same social phenomena through this technology and live their childhood through it. There, the difference is in what this mediation causes to their experiences.[14]

## 2.3 Children's digital safety

Since the proclamation of the Convention on the Rights of the Child, and with the spread of the Internet and technological media, the societal landscape has changed completely. Estimates suggest that one in three users of the Internet is under eighteen years old.[15] On the one hand, information and communications technology (ICT) has made it easier for children to exercise their rights in a way that allows their potential and abilities to mature and flourish through social communication and interaction, learning, access to vital sources of information on issues that will impact their lives and communities, and expressing their opinions.[16] Nevertheless, the use of technology by children has created a range of challenges and risks, such as: invasion of privacy, exposure to inappropriate content, bullying, sexual grooming and exploitation, human trafficking, and discriminatory algorithm policies in digital platforms, in addition to paving the way to new ways to harm or commit violence against children.[17] It was not until 2021 that an official declaration was made to keep pace with all these developments, when the Committee on the Rights of

12. Livingstone, Sonia; Blum-Ross, Alicia. (2017). "Researching children and childhood in the digital age." In: Christensen, Pia; James, Allsion. (Editors). Research with children. London: Routledge. Pp. 66-82.
13. Livingstone, Sonia; Blum-Ross, Alicia. Ibid.
14. Livingstone, Sonia; Blum-Ross, Alicia. Ibid.
15. Livingstone, Sonia; Carr, John; Byrne, Jasmina. (2015). One in three: Internet governance and children's rights. Center for International Governance Innovation. Retrieved in (19/02/2024), from: Click.
16. International Telecommunication Union. Whoa, who Child Online Protection: Guidelines on Child Online Protection: Keeping Children Safe Online. Retrieved on (December 19, 2024), from: Click.
17. The United Nations. (ND). *Convention on the Rights of the Child: General Comment No. 25 (2021) on the rights of the child in relation to the digital environment.* Retrieved on (19 December 2024), from: Click.

the Child (CRC) issued General Comment No. 25, which specifically addresses children's rights in the digital environment. The comment obliges countries of the world to protect and respect children's rights enshrined in international and local laws in the digital sphere as well.[18]

## 2.4 The Palestinian children

Israel views Palestinian children as a "problem" that could change the demography of the ruling majority. One of the means Israel uses to manage this "problem" is controlling the legal status of children. In 2012, nearly 156,985 children living in Israel were registered as stateless, with more than 75% of whom reside in Jerusalem. In this way, Israel places children in a state of "unauthorized legality," especially since living without formal legal status imposes restrictions on children in mobility and access to educational institutions and medical services, which may put their safety and livelihood at risk.[19]

Nadera Shalhoub-Kevorkian describes Israeli policies toward Palestinian children as aimed at "stripping them of their childhood" by defining them in security terms, such as dangerous, criminals, potential terrorists, or racialized others,[20] allowing Israel to commit brutal political violence, exclude Palestinian children from the sphere of childhood, and infringe their rights. These discourses transform Palestinian children from human beings into unwelcomed illegal or illegitimate bodies. Needless to mention that this discourse grows in periods of wars and confrontations.[21]

## 2.5 Childhood in East Jerusalem

Children in East Jerusalem are extremely affected by political persecution and social deprivation as they are discriminated against based on their race, nationality, political affiliation, and religion. In producing this reality for Jerusalemite children, three discriminatory systems intersect, thus, limiting their chance of improving their lives and future well-being:

1. Lack of government assistance and support; both the Israeli and Palestinian systems shirk social and legal responsibility towards these children
2. Limited access to social welfare, justice and education opportunities
3. Structured discrimination that classifies Jerusalemite children as criminals or as a security threat.

18. Livingstone, Sonia; Carr, John; Byrne, Jasmina. Ibid.
19. Shalhūb-Kīfūrkiyān, Nādirah. (2015). *Security theology, surveillance, and the politics of fear.* Cambridge University Press.
20. Racialized persons are those who are racially labelled based on race.
21. Shalhoub-Kevorkian, Nadera. (2019). Incarcerated childhood and the politics of unchilding. Cambridge University Press.

As a result of this fragile social and political reality, Jerusalemite children are deprived of basic services and their basic needs are not met due to the lack of access to public services, including health, education, social welfare, water systems, infrastructure and sanitation systems.[22] According to the estimates of the Jerusalem Center for Economic and Social Rights, 80% of Jerusalemites live below the poverty line during the past two years.[23]

Moreover, there are many cases of political violence by Israeli law enforcement and judicial agencies against children, followed by additional measures of deprivation, isolation and imprisonment, rather than securing care and protection.[24] Indeed, Israel killed approximately 25 Jerusalemite children within four months of the outbreak of the war on Gaza.[25] In addition, 350 children over the age of twelve and 35 children under the age of 12 were arrested after October 7th, 2023. As for the charges for which Israel has tried and prosecuted children, some fell under the Anti-Terrorism Law on charges of inciting on social media or participating in confrontations that erupted at the beginning of the war between Israeli forces and residents in sporadic areas in Jerusalem.[26]

## 2.6 Digital rights of Palestinians

Previous studies by the 7amleh Center on the digital safety of Palestinian youth and children in the 1948 area,[27] the West Bank, and Jerusalem have shown that the digital landscape is characterized by the structure, complexity and an accumulation of violations and their sources, in which the Israeli occupation, technology companies, official Palestinian bodies, society and private commercial companies participated. Therefore, after the Palestinian virtual space has become subject to censorship policies in the same manner that the digital life of Palestinians is subject to the occupation's military measures and permanent censorship, Dr. Saeed Abu Ma'ala believes that the framework for analyzing the Palestinian real landscape is cyber-colonialism, as it became impossible to separate the concept of colonialism on the ground and colonialism in digital spaces.[28]

Given that the Internet was not designed from the outset in a way that considers the safety of children, these violations are expected to carry a double and deeper risk to the lives of Palestinian children. Thus, their rights are at the forefront of direct digital threats

22. Kovner, Bella. Ibid.
23. Al Jazeera Net. (2024, February). Poverty in Jerusalem... The circle is widening and there is no horizon to narrow it. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
24. Kovner, Bella. Ibid.
25. Al-Rajoub, Awad. (2024, February). 29 martyrs in Jerusalem, half of them children, since October 7th. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
26. Al Jazeera Net. (2024, February). On their International Day... Children in Jerusalem are tortured inside and outside prisons. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
27. Abu Ma'ala, Saeed. (2024, August 28). Digital Security Among Palestinian Youth Citizens of Israel: A Study on Threats and Challenges in Light of the War on Gaza. 7amleh Center. Retrieved on (19/12/2024), from: Click.
28. Abu Ma'ala, Saeed. (2024, August 28). Digital Security Among Palestinian Youth: A Study on Threats and Challenges in Light of the War on Gaza (West Bank and Jerusalem). **7amleh Center.** Retrieved on (19/12/2024), from: Click.

in the network.[29] Indeed, a study conducted by 7amleh Center in 2022 showed that 87% of Jerusalemite children refrain from digital expression and political participation through social media platforms, while 58% believe that they are subject to censorship by the Israeli authorities. In addition to violations on a political basis, another type of abuse that is of concern to children and their families is attacks from the social environment of children, which included verbal violence (58%), bullying (42%) and blackmail (13%). Moreover, 10% of the female respondents reported they were subjected to sexual harassment.[30]

Considering their knowledge of digital protection tools and means, it was found that 45% of Jerusalemite children are keen to change the settings of their accounts on social media platforms periodically to protect themselves and their privacy. Children and their caregivers, including parents, counselors, and teachers, expressed an urgent need to develop their knowledge about digital safety to protect their devices and children.[31]

# 3. Objectives of the study

The current study explores the experiences of Jerusalemite children aged 12-18 with the digital environment and digital security management, focusing on the following axes:

1. The extent to which Jerusalemite children are aware of digital risks and threats, as well as protection tools and techniques necessary to maintain their digital safety.
2. Identification of parties that pose a threat to Jerusalemite children's digital safety, i.e. Israeli forces, colleagues and peers, family members, acquaintances, and strangers.
3. Identification of the parties to which children resort for support and assistance when they are exposed to digital violations, and the effectiveness of these parties in providing such support.
4. The role of social actors and caregivers, such as: parents, school staff, and employees of civil society institutions in children's digital safety.

## 3.1 The importance of this study

The wide and essential presence of electronic devices in children's lives means that they have come to play a crucial role in their mental, emotional and cognitive development, which requires us to pay special attention to the effects of these devices on them at this developmental age, when mental plasticity is at its maximum. In addition, especially during crises and wars, digital and technological innovations are affecting the lives and rights of children in broad and interconnected ways, as all social and life services depend

29. Miller, Steve. (2024, February 23). Child protection in the digital world: Why it is needed. **Save the children**. Retrieved on (19/12/2024), from: Click.
30. Berekdar, Mohanad. (2020, September 29). Digital Safety Among Jerusalemite Children and Youth. 7amleh Center. Retrieved on (19/12/2024), from: Click.
31. Ibid.

on these technologies, including education, government services, trade, etc.[32] Therefore, it becomes essential to study the effects of the use of the digital environment on the lives of children, and the extent to which children are provided with opportunities to exercise their rights. We also need to explore the conditions and contexts that hinder children from exercising their rights, and the parties responsible for these barriers to improve the experiences of children and enable them to benefit fully and comprehensively from these technologies.

Furthermore, understanding the role of caregivers, parents, counselors and teachers is critical in shaping children's cognitive, emotional and social development.[33] To complement our understanding of children's digital experiences, it is essential to understand the role of adults in mediating the relationship between children and technology, and in guiding children on beneficial use of technology and basic protections measures. Since children tend to adapt to the digital world faster than caregivers, it is particularly necessary to understand the needs of parents to enable them to better guide their children, as they bear part of the responsibility for their children's digital safety.

# 4. Methodology

The study relies on data analysis from three focus groups with children, three focus groups with children's caregivers, and data from six action groups of children that 7amleh Center has previously worked with. The groups are as follows:

## 4.1 Focus groups with children:

The duration of focus groups with children ranged from two to three hours, while the number of respondents in each group ranged from 6-13 children. The total number is thirty children from the following areas in Jerusalem: Issawiya, the Old City, Sheikh Jarrah, Wadi al-Joz, Jabal Mukaber, Silwan, Ras al-Amud, Beit Hanina and Shu'afat refugee camp. The study considered the ethics of research with minors by communicating with the children's parents and obtaining from them consent for their children's participation, either by phone or written. During every focus group session, the researcher informed the children about the course of the study and their rights throughout, to ensure their informed participation in it. Data collection and the coordination of the groups faced many difficulties. Most notably, the need to reprocess sensitive data shared by children when presenting it in the study to ensure full protection of the children and their families. In addition, the study relies on analyzing data from six groups of children with whom 7amleh center worked during the months of May-June 2024, seeking insights from them for the current study.

32. The United Nations. (ND). General comment No. 25. Ibid.
33. Ibid.

## 4.2 Focus groups with caregivers:

Three focus groups with caregivers of children were conducted: one with parents of children (7 respondents: five mothers and two fathers), one with civil society employees in Jerusalem (4 respondents), and one with school staff in Jerusalem (4 respondents). We received consent from all respondents.

In all groups, information was collected by recording the focus groups' discussions, transcribing them, and deleting recordings after transcribing. Subsequently, data were scanned through Atlas.ti and thematically analyzed based on topics that were repeated in most groups.

# 5. Results and analysis

## 5.1 General note

Interviews with activists in Jerusalem's civil society revealed that institutions cannot yet be preoccupied with Jerusalemites' digital safety, while a good percentage of the population suffers from poverty, illiteracy and a lack of other necessities, including the shortage of electronic devices, "for example, there are basics that must be fulfilled. I cannot teach about digital safety when people do not have computers, they do not have devices. No, there are basic needs before I talk about digital safety"; "[...] Not all people have financial means. Covid required families to have modern technologies. However, not everyone had them". Naturally, this situation prompted the organization to open a computer lab equipped with a limited number of computers, not more than ten devices.

## 5.2 Children's social environment and digital violations

This section reviews the digital assaults that Jerusalemite children are exposed to from their social environment. It addresses the most crucial factors that affect the level of digital safety of children, and the harms and negative effects of them. Firstly, when children shared their sense of digital safety, their experiences and attitudes were divided into four categories: the first group links the level of digital safety to internal feelings that they rely on to determine if anyone is watching them in the digital world – "It's normal, I don't feel that someone is watching what I am doing" – without any consideration that inner feelings are not a reliable measure of how secure they are digitally. The second group of children links children's sense of safety to their behaviors in the digital environment and

do not see the necessity to feel insecure as long as they do not engage in "bad" practices – "The same thing with me... I do not make anything wrong on the phone." This group does not take into account that risks and threats do not necessarily stem from bad behaviors committed by in children, but rather from the intentions of the abusers, who do not necessarily have good intentions when committing digital violations, as well as from the way they use the children's data once it falls into their hands.

The third group of children have lost the sense of security when using electronic devices at all, carrying with them a constant and intense fear of being monitored throughout their use of technology – "I, too, do not feel safe, because the world has developed and technology has become smart, and everyone is using it...", "It is not safe... the phones are always monitored". The fourth and final group of children feel partially safe. Their feelings stem from believing that some apps are more secure than others, or that they are not easily hacked, "There are many groups on Telegram [...] [Israel] cannot hack the factions' channels", "I don't think all the sites are monitored...", "WhatsApp is less [monitored]..."

### 5.2.1 Cyberbullying:

Cyberbullying phenomenon is common among children in Jerusalem. Although the causes of this phenomenon vary, the children's creativity in using technical means to practice cyberbullying takes a new form, different from bullying in real life. Just like bullying in reality, most cyberbullying incidents among children are related to external appearance. This specific type of bullying relies on "beauty" standards set by society for both males and females alike, which are reinforced by social media by intensively emphasizing and focusing on visual and external effects. The digital sphere enables rapid spread of violent content and reaches large audiences, deepening the impact of bullying on child victims by publicly shaming them. This type of bullying may create among children complex relationship with their bodies later in life. Some female respondents indicated that at times female classmates preferred not to return to school because they were unable to confront their classmates after the cyberbullying content reached all school students.

### 5.2.2 Extortion, threats, and publication of images:

The most common phenomenon in the stories of Jerusalemite children is extortion. The assailant is usually a male and the victim is a female, while the means of extortion is use of personal photos of the females. The way the extortioner obtains the photos varies. In certain cases, females voluntarily share photos or passwords of their personal accounts with males with whom they are in a friendly or love relationship. If a password is shared, the extortioner may have access to photos shared by other female friends – "This happened to me once... My friend wears a hijab, but she posts streaks without it. One of her friends gave her boyfriend the password to her account, who kept texting her from her friend's account, pretending to be her, saying, 'How are you, beautiful?" Nonetheless, some females are subjected to hacking of their accounts, or to being photographed on the streets or at their school, home, etc. Finally, a common phenomenon among males is creating fake accounts with fake names to lure other young males or females to share sexual images and then extorting them.

The aims of extortion among children are often limited to receiving payments in exchange for refraining from publishing the images, or winning a bet, or even merely for entertainment or getting other requests carried out by the victim. In one case where a female was the assailant, the aim of her extortion was preventing her boyfriend from leaving her by threatening to publish images that may lead to his legal incrimination. This kind of threat and extortion goes beyond ruining a boy's reputation or his image in front of the society, to threatening his freedom.

In a serious incident, the assailant was an adult woman, and the victim was only a ten-year-old boy. The boy was sexually harassed by his teacher while she documented their "sexual activities" and sent the video to his parents to blackmail and get funds from them. However, the child's parents decided to publish the video themselves to protect their child and draw the boundary between sexual harassment and indecent conduct. As a result, the teacher lost her position and paid a toll for her actions.

### 5.2.3 Identity theft:

Identity theft is the second most common child abuse. In some cases, the children are the victims of identity theft, and in others they are the assailants. The most common incidents of Identity theft against children are by using a fake identity of a young female or male to entrap children. In other cases, the assailant steals the identity of the victim to commit heinous acts to damage their reputation or distort their societal image or

ruin their social relationships with others. For example, the identity thief sent slurs to the victim's acquaintances or sold drugs in his name. When the victim is a female, the aim of stealing her identity is usually connected to attempts to damage her honor and reputation, especially in matters considered a social and cultural taboo. For example, stealing the identity of a young female and flirting with other young males or chatting with them on intimate issues. In one case for example, an adult created a fake identity of a football coach to lure young boys and sexually assault them. In other cases, children steal identities for personal gain from people around them, such as their parents or teachers, by tricking them into sharing personal information that can be used against them in the future.

### 5.2.4 Spreading misleading and fake news:

Fake and misleading news can quickly spread in the digital world before having the chance to validate or fact check them. Children may be victims of this kind of news because it affects their awareness, knowledge, and the extent to which their fact system is accurate, especially when conflicting information circulates on social media platforms. On the other hand, children are often the subject of fake news, which may weaken their relationships with their families or community, or worse, cause family disputes in Jerusalem. One of the girls shared an incident in which a person spread fake news about her sister's death, which caused great confusion among family members and caused panic among them until they succeeded in communicating with her to ensure her safety.

### 5.2.5 Stealing accounts/phones and "hacking" of electronic devices:

It seems that stealing each other's accounts in social media and games is a widespread phenomenon among Jerusalemite children, indicating that children are unable to maintain the lowest levels of digital security in protecting their accounts. As one of the female respondents mentioned above has indicated, hacking accounts does not necessarily mean that only the account holder is affected by the hack as it may result in access to sensitive information shared with the account holder by friends. Secondary victims do not consider that the hack may not have originated from their own phones or accounts, and that the Internet is a network of relationships and accounts. If one account is hacked, this means that part of their information will also be leaked.

A respectable number of child respondents in focus groups bragged about their ability to repeatedly "hack" websites and digital accounts – "I have 12 accounts, all of them stolen." In a strange incident, a child in the age of primary school "hacked" another child's device. His teacher shared, "A boy hacked his peer's device completely. We can describe it as a family computer. The administration of the school intervened in the matter because the boy was able to have access to things or pictures that he was not supposed to see." When asked about the reason for the child's action, she answered, "There was an accumulation of trouble between the two kids."

Children steal accounts by issuing a SIM card with the same number the account is registered (with the help of acquaintances and friends working in this field) and later reset the password through a code that they receive with the phone number (Two-Factor-Authentication (2FA) linked to a text message). Therefore, educating children about the importance of using open-source authentication applications is crucial, such as OTP Auth, since 2FA linked to a text message has become insecure and easy to intercept. Finally, young male respondents shared that as a result of their experience, they are responsible for creating and securing accounts of family members. However, a substantial percentage of them keep the login details and can access the accounts at any time.

### 5.2.6 Violations and assaults via digital games:

A special section of the study was dedicated to these kinds of violations due to the substantial number of violations children are exposed to through online games, as well as parents' concern about the risks associated with online games. Large numbers of testimonials were associated with financial theft via online games, either by luring and deceiving children, or by hacking accounts and accessing digital wallets or bank details linked to the accounts. In addition, children are indifferent to the reliability of the gaming apps they use. Adults described some of these apps as "semi-spy games"[34] capable of hacking into the phone's data systems and accessing children's personal and confidential data and information. In addition, parents expressed their worry about children opening the camera and microphone while playing with their friends without any regard for the privacy of the family or home, especially since some of them discovered that their children communicate with much older strangers during play.

These results prove that children are exposed to digital risks associated with their increased use of electronic games, which may have both technical and social consequences. As for technical consequences, anonymous games (i.e., games without a verified source that may be accessed by cracking)[35] may contain multiple malwares.[36] The least harmful and most

34. To see a list of games that use similar systems:
Wired. (2023, July 17). Video games, data privacy, and artificial intelligence. **Wired**. Retrieved on (2024, December 24), from: Click.
35. Wikipedia. (n.d.). *What is software cracking*. **Wikipedia**. Retrieved in (December 24, 2024), from: Click.
36. Perekalin, Alex. (2020, April 3). The dangers of cracked games. **Kaspersky**. Retrieved in (December 24, 2024), from: Click

common are games that contain software that displays advertisements on the device, both during and outside of gametime (Adware.)[37] When these games cause more damage, they may contain software that records every button press made by the user and then sends it to the assailant (keylogging.)[38] Moreover, some software may collect all data about the devices and send it to the assailant, who may threaten the owner of the device and push him to carry out any requests. In worse cases scenario, the malware may fully control the device with all data encrypted in it, before demanding from the owner of the device a ransom (ransomware.)[39]

Reliable electronic games may exploit the powers granted to them by using anti-cheat programs called kernel privileges, which only work in computers. These programs are able to monitor and control all the user's behavior in their device, thus, tremendously empowering them to combat cheating. The real danger lies in the case someone is able to find a software loophole in this type of program, allowing them to use it to fulfill their goals without any objection as a result of the powers granted in the agreement. In theory, the manufacturers can acquire whatever data is in the device they want as a result of the powers granted to them in the agreement.[40] Example for this type of cheat programs:

- **BattleEye** used in games like **Rainbow Six** and **Siege**.[41]
- **Riot Vanguard** used in **League of Legends** and **Valorant**.[42]
- **Easy Anti-Cheat** used in **Fortnite** and **Apex Legends**.[43]

The social consequences are no less serious than the technical. Children's contact with other players can have profound consequences, including: Doxxing,[44] i.e., leaking personal information (e.g., home address, social media accounts, parents' work location, etc.), which can lead to devastating consequences for children. Astonishingly, the least harmful consequence is cyberbullying.[45] For example, sending anonymously unsolicited parcels to the child's address. The most dangerous consequence is filing false reports about the child's home, causing a raid on his home (swatting),[46] or communicating with the child's parents' workplaces to submit fabricated reports about them, which may cause them losing their job. The most serious of these consequences is causing physical harm to the child or his acquaintances by tracking his movements (Stalking),[47] or perhaps assaulting him near his home, school, on the street, etc.

37. Kaspersky. (n.d.). What is Adware?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
38. Kaspersky. (n.d.). What is a Keylogger?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
39. Kaspersky. (n.d.). What is Ransomware?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
40. Conway, Adam. (2022, April 15). *Dangers of Kernel Level Anti Cheats*. XDA Developers. Retrieved in (December 24, 2024), from: Click.
41. Wikipedia. (n.d.). *BattleEye*. **Wikipedia**. Retrieved in (December 24, 2024), from: Click.
42. League of Legends Fandom. (n.d.). *Riot Vanguard*. **League of Legends Fandom**. Retrieved in (December 24, 2024), from: Click.
43. PCGamingWiki. (n.d.). *Easy Anti-Cheat*. **PCGamingWiki**. Retrieved in (December 24, 2024), from: Click.
44. Cruz, Brett; Turner, Gabe. (n.d.). What is Doxxing?. **Security.org**. Retrieved in (December 24, 2024), from: Click.
45. Kaspersky. (n.d.). Top 10 ways to stop cyberbullying. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
46. Cloudflare. (n.d.). What is Swatting?. **Cloudflare Learning Center**. Retrieved in (December 24, 2024), from: Click.
47. Kaspersky. (n.d.). How to avoid cyberstalking. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.

Before reviewing other digital assaults and abuses, it is important to note that the reasons why children commit attacks against each other, their peers, friends, or classmates in school can be categorized into four motive: First, revenge; following the accumulation of feelings of anger, resentment or annoyance with other children that have not been resolved or addressed gradually. Digital abuses may aim to demarcate power relations between children, so that cyber violations will be disciplinary measures for their colleagues to "stick to their limits" in the future. This type of abuse shows that children do not know how to manage their feelings and conflicts with each other or ask for help from the adults around them. Therefore, the act of revenge and its consequences are much greater than the mistake caused by the child victim in the beginning. Consequently, there is a need to work with children to equip them with the basic skills to address their personal problems and conflicts in the right and peaceful way.

The second motive for committing these violations against each other is to defame the victims. The third and most frequent motive mentioned by children was entertainment: "[...] he was mocking him. He did not shame him, I swear. Only having fun," "we used to do this when we were kids, we were just having fun," "no, it is not [ransom], it is only for fun. That is it," "I'm just kidding with her..." "just for fun, this is what we felt like doing..." This data is extremely worrying. Children have fun by flexing their "technological muscles" and find hacking (unauthorized access)[48] other people's devices and accounts or even causing harm to them to be funny. This motive reveals a deeper ethical dilemma related to children's behavior, and the other side of the coin, when children are complicit to the attacks, and not passive victims.

### 5.2.7 Exposure to inappropriate content:

Jerusalemite children, especially children at the early age, are frequently exposed to inappropriate and pornographic content. This type of exposure is sometimes unintentional and occurs through advertising, content suggestion and recommendation system, and automatic content transition on social media sites. This phenomenon causes great concern among parents and other caregivers. A parent respondent shared, "I can see what he watches on YouTube. He watched horrendous things, I mean, things inappropriate to this age, things that 16 or 17 years-old youth watch." On the other hand, some parents indicated that they do not mind children watching suggestive content – not pornographic – as long as they do so at home under their supervision, so that they have the ability to guide them. As one mother put it, "I prefer that they know what is right from

48. See: https://techterms.com/definition/hacker

me rather than learning from an outside source." Some youth, even at the primary level, choose to consume digital sexual content out of curiosity, or, as one teacher mentioned, because they "consider this the freedom they are deprived of. It is natural that they will covet the forbidden."

### 5.2.8 Censorship by community members:

Children describe a wide range of practices in their social environment that monitor their behaviors in the digital or real world, and consequently, report these behaviors to their parents. For example, a neighbor filmed a boy smoking a hookah and shared the video with the boy's father. In other cases, girls may post a "story" about a visit to a certain place, and others may report this visit to their parents which may instigate a confrontation with the parents. All children in the focus groups expressed discomfort regarding this behavior and consider it a violation of their privacy that restricts their freedom. In addition, they do not think that strangers have the authority to interfere in their affairs, "[It is] that important to him, although he does not know him at all," "why [do they tell their parents]?" "What do they have to do with it?" "No, I don't care that they told them [the parents], but why did they do so?"

The members of the Arab society behave as collective caregivers of children, as if children were a collective social property that every member must contribute to their "education," guide their behaviors, and ensure it is in line with social expectations. This kind of behavior is related to the nature of Arab societies, which are characterized by high societal density and intertwined relationships; it is precisely what annoys children and makes them feel suffocated. Therefore, children use possibilities offered by technology to avoid censorship. For example, "I blocked my aunt," "I have to hide or block them," "I didn't block them, but if they sent me a follow request, I wouldn't accept."

### 5.2.9 Electronic financial fraud:

Some children have been targeted to get their own, or their parents' financial or banking information. This is done by electronic phishing with false messages that trick them into providing their banking information, "You know these links that say 'buy with one hundred shekels and win with us... They steal your credit card number...." Another method of phishing is through fake websites or pages aimed at luring children to provide them with their bank details, "there were some people who opened a fake page through which they offered buying an iPhone in 5,000 NIS instead of 7000 NIS. He ordered the mobile phone, paid by Visa, but he received a Nokia phone that came in an iPhone packet."

On the other hand, the study reveals that digital fraud is widely common among children through stealing the financial identity of lost credit cards in Jerusalem. Some children did not physically touch a credit card and only photographed its details from both sides. In other occasions after using credit card details in games for the first time with the approval of their parents, some children may reuse the details they have saved without their parents' consent, and for unlimited amounts. Moreover, children often deceive their parents by telling them their accounts have been hacked to hide their behavior.

### 5.2.10 Malicious links:

Malicious links have been mentioned a lot in children's testimonies about the digital violations they are exposed to. A large number of Jerusalemite children's devices and/or social media accounts are exposed to hacking as a result of clicking on certain links, "Links... Links... Many many links... Even when a message comes from some website [...]" and "my phone is hacked a lot... A lot... By God, I do not know who hacks it exactly... But I was getting links...." The content of the messages children receive aiming to trick them into clicking on these links varies: advertisements to promote the purchase of a specific product at a discounted price or participation in a competition to win a sum of money. Some of these messages try to exploit humanitarian or religious issues in order to manipulate children's emotions and push them into clicking the links. Children often fall into this trap and drag others as well, "Some of them send a message pleading for Gaza, saying: 'enter here to help them' etc., then they hack your account," "I would like to tell you that they use it for religious reasons as well, they may send prayers [...] spread the link to earn a spiritual reward."

## 5.3 Attacks on political grounds and after the 7th of October

### 5.3.1 Attacks by Israeli forces and authorities

### 5.3.1.2 Censorship techniques:

Although access to the Internet and the use of electronic devices is one of the basic rights of citizens, this access also means that users are leaving behind electronic fingerprints and traces of many of the social interactions and practices they engage in. These electronic fingerprints necessarily mean that they can be tracked and traced.[49] Indeed, the results of the study indicate that Jerusalemite children feel all the time that "everything, everything is monitored," or "the phones are always monitored, and anything we watch, and when anyone calls us, they always know, even if it was something

49. Livingstone, Sonia; Blum-Ross, Alicia. Ibid.

unrelated to politics." Children feel that there is a hidden person present in their lives, accompanies them at all times of their day, knows everything about them, invades their privacy and lives, records all their details and persecutes them through it. According to a child respondent in the focus groups, "they monitor everything you do on social media as well; they know everything... even what you search for, how you walk in the street, they can recognize you from your clothes, your shirt, your boots..." This description reflects the vision of a superhuman, someone who has extraordinary superhuman abilities, a kind of digital deity present in their lives with the presence of electronic devices regardless of whether they are used or not, "when I am in my house even if [I am] not using electronic devices, as long as they present [I am not safe]."

This surveillance and absolute knowledge of everything provide the Israeli authorities with pretexts to deprive children of basic rights, such as their freedom, privacy, and dignity. For example, respondents in the focus groups shared that some families live in the West Bank even though they are citizens of Jerusalem. If the Israeli authorities discover this, they may threaten to strip them of citizenship or residency, or even health insurance, national insurance services, and education. Tracking and monitoring the geographical location of children is done either through GPS tracking, or even their Rav Kav card (a digital public transport card). This card keeps the user's complete travel history, boarding points, and disembarkation points as well.

#### 5.3.1.2 Arrests, interrogation, and home detention of children:

Arrests of children, and adults as well, was present in the children's group discussions, "anyone who publishes anything on social media gets arrested." Some of the stories shared are related to first-degree relatives, such as siblings or cousins, or more distant relatives. Some Children who participated in the focus groups have been previously investigated or arrested. In other cases, classmates or close friends of the respondents were arrested. Generally, the charges against them were, "liking a post about Palestine," or even reading content Israel classifies as a content that supports terrorism, or even because of putting a black profile picture on WhatsApp, which Palestinians use as a symbol of mourning for the dead of Gaza, and solidarity with its people. In addition, Jerusalemites were arrested for publishing Quranic verses or prayers, even if they are related to their personal lives and not to war. Children shared that some of their acquaintances were arrested for joking with each other in the WhatsApp group with phrases like "O' we are being bombed," when Iran attacked Israel by missiles and some rockets fell in Jerusalem. This kind of arrests reflects the absurdity of the Israeli legal and police system in targeting Jerusalemites, classifying

any words or phrases related to Palestine, war, or Islam as necessarily terrorist, even if the context of their use is not related to the ongoing war, and even if they were used to ridicule. The punishment to these arrests outweighs the severity of the "crime," such as liking a post. Thus, these practices dilute the discourse of human rights and international laws.

The arrest of children in East Jerusalem is primarily a political and racist act, and a form of slow violence practiced by Israel against Jerusalemite children because they represent the continuity of Palestinian existence and survival in Jerusalem. In addition, Palestinian childhood is targeted because it inherently embodies of wider scopes of freedom, liberty, curiosity, and boldness before children learn to fear. As the paper will show later, the authorities try to eliminate these qualities to instill fear in children, with adults playing a significant role in passing down the legacy of self-censorship and a deep-seated fear of the police system.

### 5.3.1.3 Phone inspections:

Since the seventh of October 2023, the phenomenon of phone inspections has been expanding, as more than sixty stories about this phenomenon have been collected during the focus groups. The Israeli soldiers thoroughly inspect all messages and social media applications on children's phones (Facebook, TikTok, WhatsApp, Instagram, YouTube), while paying special attention to the Telegram application and the channels that the child follows in it. In addition, photos and videos in the phone, archives, recycle bins, and even the phone covers themselves were inspected frequently. As for the magnitude and level of this phenomenon, as some children have pointed out, "[...] Every school student's phone would be inspected, also his bag and so on." Some female students referred to mass inspections of children at bus stations after school hours. In addition, soldiers might inspect the passengers of an entire bus, "they would ask all the passengers to get off, search the girls, the guys, everyone..." Most respondents agree that males are more likely to have their phone inspected than females. This may be related to the perception that males may engage in "terrorist," "resistance," or "hostile" acts.

Children are particularly exposed to phone inspections in the following cases: The Israeli police carry out raids on schools to inspect students' phones, and sometimes even electronic tablets used for studying purposes. According to child respondents, these raid cause panic and trauma among students, teachers and administrative staff.

Phone inspections are also frequent at checkpoints when children return from the West Bank to enter Jerusalem, or in other new checkpoints placed by Israeli forces since the seventh of October at the entrances to some neighborhoods and towns in Jerusalem. In addition, phones are inspected at all gates and entrances to the Old City of Jerusalem, especially Damascus Gate.

Over time, children have developed some tools and mechanisms to deal with these inspections, starting with deleting the Telegram application completely, or deleting it periodically before passing through the checkpoints. In addition, some children indicated that they now refrain from carrying phones at all while passing through checkpoints. Some schools have banned bringing phones to school to avoid inspections.

Phone inspections are accompanied by a wide range of violations of children's rights and dignity, especially as they threaten their safety and disrupt their daily routines. These violations include confiscating phones without a warrant or legal basis; beatings of male participants in particular, threats, and even arrest following an inspection of their phones. Some children were threatened by soldiers with their weapons. Children are subjected to additional inspections associated with phone inspections, such as searching school bags, books, clothes, and body searches. Some children were stripped naked or asked to undress. In other cases, Israeli soldiers smashed children's phones as punishment, while some deliberately detained children for extended periods at checkpoints, up to an hour of waiting. These attacks constitute a violation of the most intimate spaces and experiences of children, by completely violating their bodies, places of study, residence, and homes. This complex machine of violence brings with it a simultaneous comprehensive violation of a large part of children's rights.

### 5.3.1.4 Self-censorship:

In accordance with previous studies conducted by 7amleh Center that show that Palestinian youth from all geographical areas practice self-censorship, children's testimonies and statements in this study indicate that the same behavior is observed among them. Jerusalemite children refrain from posting, liking, sharing, or even watching content related to the war and genocide in Gaza. The difference between the findings of this study and previous studies is that most children are now self-censoring due to social pressure by the adults surrounding them. The impression is that adults and caregivers play the role of security officers with their children. The respondents received a wide range of instructions and guidance from adults in their surroundings to refrain completely from any interactions with political content in the digital world. For example, many of them

reported that school administration and the counseling staff entered the classrooms one by one with instructions, “No one shall post or write anything or post any comments,” “they told us not to post anything about Gaza.” Parents exercised strict control over their children in this regard. Some expressed that the challenge of protecting their children on political grounds outweighs any other digital risks they had to deal with. Therefore, some parents prevented their children from publishing any political posts. Caregivers explain that playing the role of the officer stems from fear for the children and their desire to protect them from arrest and accountability because this responsibility falls on their shoulders. They also testified that playing the role of the officer was painful for them, especially because they wanted to preserve the children’s sense of patriotism, ““My feelings with them were very mixed. I cannot put this emotion in any frame.”

Despite all the mentioned controls and restrictions, children were not deterred from posting. Female respondent said, “[...] I stopped for a while, but eventually I posted again, although it was not like before,” “they seriously thought that if they arrest someone from our area that we will be afraid and stop posting, but we are not afraid, everyone posts as they wish.” In one case, a student refused to open his phone for inspection because he did not delete political material from his phone as directed by his father and school staff. These examples are proof that children are eager to exercise their right to expression and their right to political participation, and to exercise their moral role towards their own people. Childhood in Jerusalem becomes a political stance. Due to circumstances and political context, childhood is no longer bound to a its traditional role. Rather, childhood enters the field of activism with a vision of change, as one girl said, “[...] why are we preventing ourselves from posting just because we are afraid? What we are going through is nothing compared to the people of Gaza.”

### 5.3.2 Technology companies:

Restrictions on children's rights were not limited to Israeli and societal policing practices. Child respondents addressed the issue of digital platforms that played a significant role in thwarting and curbing children's political activism through many techniques and methods. Before delving into the role of global digital companies in this process, it is worth noting that the children expressed great concern about the fact that the telecommunications companies that provide them with their services are all Israeli, “all these companies are affiliated with Israel. Thus, they do not need to hack the phone to monitor you.” Palestinian telecommunications companies are not allowed to provide Jerusalem residents with their services, which constitutes a fundamental problem for Jerusalemites.

Children point to many violations Global companies commit against them:

1. First, Jerusalemite children feel discriminated because global platforms restrict their interactions and discourse while they do not restrict Israelis in the same manner. In addition, global platforms contribute to spreading misleading and fake news by the Israelis.
2. Many children have been banned or restricted on their accounts or publications, and some content was deleted. One of the restrictive techniques mentioned by children is shadow banning, i.e., reducing the number of views on their posts or restricting interaction on them, or classifying them as sensitive content.
3. The platforms restricted children's right to access information by placing warning signs for posts supporting the Palestinian cause and classifying them as dangerous or sensitive material, or through algorithmic manipulation of search engines to favor specific content over another, or even blocking content related to the Palestinian cause.
4. By deleting hashtags that support the Palestinian cause or shutting down Palestinian groups on social media, the platforms violate children's right to digital assembly.
5. Algorithmic bias for digital applications hinders the freedom of movement of children and their parents. Children complained about constant warnings in Waze app when entering areas in the West Bank, or even failing to provide updates regarding closed checkpoints, thus prolonging the route.
6. These platforms violate children's right to privacy through targeted ads that target them based on their preferences or private conversations with their friends.

In any case, children are not passive users of social media. In turn, they try to circumvent the algorithms by using lingual encryption with certain symbols, or even use alternative Palestinian applications, such as “Azma” application, which displays traffic crises imposed by checkpoints.

The children shared difficult and complex emotions regarding the impact of these discriminatory policies on them, “in principle, of course one must share content, because what happens with us is nothing compared to what is happening to them [in Gaza], we are not able to do a small thing to help them,” “I am guilty of this thing,” “I get nervous,” “oppression,” “they [the Israelis] are not better than us, why are they allowed to express themselves while we are not?” “You feel it is not fair. There is no justice. Why? We are exactly like them,” “you feel that you want to change this thing, but you cannot,” “tied up. You still feel that you cannot do anything. It is not possible for you to make a change,” “they make you feel they are better than you, even if by little,”“We are alone, no one is standing with us,” “I feel that we are standing alone. Everyone is with Israel, and no one is with us.”

The most difficult thing that emerges in children's feelings is questioning their human value and their entitlement to life and freedom. The loss of a sense of justice in this early age may create in children an existential crises and a sense of enmity towards the world, which may prohibit them in a later stage to come to terms with the circumstances that created this sense of disability, and there will be no way to compensate them for this loss forever.

## 5.4 The role of caregivers in children's digital safety

The Council of Europe Convention states that children have the right to receive appropriate guidance and advice as they explore the digital sphere in order to ensure the realization of their rights during its use,[50] and to get the most out of these rights so that children may be able to play active role in society.[51] It is, therefore, incumbent upon states to involve relevant stakeholders in this process, in particular the education systems, child protection and welfare systems, public institutions, businesses, civil society, as well as children themselves and their parents.[52] The following section reviews the most important findings on the role of caregivers in child digital safety:

### 5.4.1 The role of the family in children's digital safety:

There is a distribution of roles and responsibility between parents when it comes to children's use of technology, just like any other behavior. On the one hand, most of children indicated that their mothers are the caregiver who is responsible for making decisions and guiding children how to use technology, because mothers often spend time at home with children more than fathers. Nevertheless, fathers, in some cases, are more involved in this process, because they represent the authority in the hierarchical structure of the Arab and Palestinian family. For example, a mother respondent said, "I failed to be an authority in this matter, especially on this issue," "[...] also, it's better if the father takes on the role of control [over the children], as I feel I'm not stern enough" Only a few respondents indicated that both parents take care of this issue together. In some cases, an older sibling may take on this role because they have the knowledge and experience needed. Regarding the role of parents in educating children digitally, parents say that proactive and conscious education at home is almost non-existent, and that it is often only addressed after children are exposed to one of the digital risks. A civil society employee noted due to their lack of digital knowledge, she noticed extreme fear of parents admitting that there was a "negligence" on their part, or that they were not performing their role to the fullest in caring for their children.

50. Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Retrieved in (19/12/2024), from: Click.
51. Economic Commission for Latin America and the Caribbean (ECLAC). Whoa, who Document hosted in CEPAL's repository. Retrieved in (19/12/2024), from: Click.
52. Council of Europe. Ibid.

When asked about the conditions and restrictions to use technology at home, most respondents indicated that the restriction is mainly regarding the duration and hours of phone use, as one parent said, “other than the time restriction, there are no laws. Nothing really.” Some children also pointed out that their families sometimes prevent them from using applications such as Telegram, Google, TikTok or PUBG for reasons related to their age, or as a result of a certain situation. One of the basic restrictions repeated in all groups is that the use of technological devices is always conditional on children finishing their homework, and that confiscating electronic devices from children has become a means of punishment for children when they make a mistake, or when their academic scores decline.

Parents use traditional and technological methods to monitor their children. It was found that some parents already use parental control apps to track and monitor their children's behaviors in the digital sphere, such as geographical location, conversations, content consumed, and hours of use of electronic devices. Parents often use these apps with younger children and stop using them when children reach adolescence. Among the applications mentioned by parents:  Google parental controls, Kaspersky, and Family Link. In addition, parents search their children's phones – with or without their consent – or as one parent said, “to be honest, one must spy on them.” However, there was a large group of children who indicated that their relationship with their parents is based on parents' confidence in their good behavior, and their confidence that their children will appeal to them when they get into any trouble. Parents used terminology of monitoring and security, while children used concepts related to rebellion, transgression, evasion, and circumvention of their parents' means of punishment and censorship. Some children mentioned “stealing” the phones back after they were confiscated, or searching for ways to cancel parental control applications, deleting all phone contents periodically, or even clashing continuously with parents and expressing annoyance and anger from them until parents give up and stop monitoring them.

### 5.4.2 The role of schools in digital safety:

The focus groups found that most schools cannot ensure digital safety, as not all have internal policies and laws on the use of electronic devices, or a protocol on how to deal with cases of digital assault, or a designated employee in the role of a digital security officer. The only policy followed in most schools is preventing mobile phones use at school and/or requesting students to deposit their devices in the morning before school hours. However, children find a way to manipulate this policy through many mechanisms.

Teaching staff and students pointed out that electronic devices in schools are old and with less capabilities than the devices used by children at home. Thus, some teachers are forced to use their own laptops at school. Moreover, some schools do not follow maintenance protocol to secure their computers or provide anti-virus or filtering software. Most teachers are expected to take this responsibility upon themselves. However, most computer teachers indicated that they do not receive any digital safety and technology training from the Ministry of Education. Absurdly, teachers need to fill in the gap and learn about these issues via watching YouTube videos, searching the web, or joining training about digital safety, mainly the training provided by 7amleh Center.

As for the role of schools in providing children with training on digital safety, half of teachers indicated that schools have never had similar workshops for students. The same allegation was repeated in the children's focus groups. However, a sizable percentage of schools affiliated with the Israeli Ministry of Education are interested in providing workshops for their students on digital safety, at least during the 'Digital Safety Month,' i.e., February of each year. Moreover, teachers criticize harshly the educational curricula in general, and the computer learning curricula in particular, which they believe have nothing to do with the reality of children as they do not provide them with mechanisms that serve them in employing technology in different aspects of their lives or maintaining their digital safety. Some teachers have also pointed out that children do not learn computers at early primary levels, although in practice, children are exposed to technology at an incredibly early age, even before primary school. Teachers attribute this imbalance in schools to several reasons, including a lack of educational resources, and a lack of awareness or disregard for digital safety by those responsible for policies in schools. On the other hand, teachers pointed out that schools can rarely deviate from instructions and directives received from the Ministry and Department of Education, which also have a responsibility for the digital safety of students.

On the other side, some private schools in Jerusalem are going through a process of digitization of education and teaching. Teachers in private schools attempt to integrate technology into teaching methods or invite private institutions and associations that provide schools with services aimed at improving and advancing students' experiences with technology. In other cases, the school administration initiates the transfer of all educational materials from books and printed papers to tablets (iPads.) However, parents and students are expected to purchase the tablets at their own expense and are expected by the school's administration to allocate the private tablet to educational purposes only through mobile device management (MDM) applied on the tablets. Students have mixed

feelings about this transition; while most do not favor the digitization of education and study, some find it to have limited advantages.

A widespread and disturbing phenomenon emerged during the study, in which the teaching staff practices different forms of violence towards students because of their digital behavior, with these violent reactions being disproportionate to the behavior of the students. Examples for students' behaviors include smuggling phones to school, photographing teachers to create "stickers" with their pictures accompanied by specific phrases repeated by teachers, or sarcastic phrases, and in one case, a racist phrase. Other behaviors include taking videos of teachers and publishing them in TikTok or Snapchat. In one case, a group of students secretly took a picture of an exam form.

The reaction of the educational and administrative staff varies and could be punitive at times, but also vindictive. In some cases, all students' phones, bags, and personal belongings were inspected. In other cases, the school may confiscate the phone for months, or even expel the student from school for days, or even weeks, or impose a blanket ban on phone use. There were incidents recorded in which teachers smashed the students' phones or complained to their parents about things the students did not necessarily commit. Other teachers called the police. Finally, it was reported that some teachers used excessive violence against the students, beating them with chairs and tools in the classroom, causing them profoundly serious injuries. The incidents further escalated because of the intervention of other parties from outside the school in the problem, as the families of the children who were beaten attacked the abusing teachers, who in turn called the help of their family members, thus, escalating the situation to an extent of using firearms. One student stated that the students witnessed a violent confrontation between the families of the two sides within the area of the school. These disputes caused casualties from both sides, and was resolved through reconciliation committees, or by paying 'Atawi' (blood money)—large sums of money paid as compensation to stop the bloodshed—rather than through police intervention.

A 2019 report on violence in Palestinian society indicates that 17% of children in Jerusalem are subjected to physical violence by a teacher, and 15% are subjected to psychological violence.[53] Professor Tayseer Abdullah from Al-Quds University discusses the factors associated with the phenomenon of violence in schools, and reveals that the percentage of violence between students and teachers reaches 66%, making it the most prevalent form of violence in schools. In his study, Abdullah points out that the violence that students and teachers are subjected to at checkpoints daily, often on their way to and from school, and the insult to their human dignity, is the primary reason behind fueling their

53. Wafa. (ND). Violence in schools. Wafa - Palestinian News and Info Agency. Retrieved in (December 24, 2024), from: Click.

anger energies that explode inside the school. Other reasons include the deteriorating economic situation of Jerusalemite society, internal societal violence from criminal gangs, imbalance in the concept of the educational relationship in Arab schools, and gender barriers that prevent males from being able to express themselves positively and restrain their emotions.[54]

### 5.4.3 The role of grassroots and civil society organizations:

All grassroots and civil society organizations have not yet developed policies and protocols to safeguard the digital rights of the children they serve, or themselves. However, all respondents expressed interest in developing such protocols because they recognize their importance. The level and type of the measures taken by some organizations to protect their devices and data ranging from not taking significant measures, to following simple procedures depending on the limited use of electronic devices in the organization and the type and sensitivity of the data they store. In addition, some organizations are already gradually integrating technology with their services and interactions with users and plan to develop this aspect further in the future. The study found differences in training staff on digital security by their organization. Some organizations did not conduct any such training, while others trained part of their staff only. Only one organization is currently training their entire staff on digital security with 7amleh Center.

All respondents indicated that they engage sometimes in conversations with children to guide them about certain uses or practices suitable for them in the digital sphere. However, no organization has ever systematically conducted training or workshops for children on digital security, nor has it ever hired an external supplier either. The organizations link their disengagement in digital security to their official mandate and specialization and mentioned that they are often bound to the desires of donors. Nonetheless, all respondents testified that there is cooperation between the different institutions in Jerusalem and that they help and support each other, including in technological issues and digital security.

All caregivers face a range of challenges and difficulties that may hinder them from performing this role optimally. An issue that was repeatedly mentioned in the interviews is the fact that they are adults in crisis themselves, as they are exposed to the same means of monitoring and control as children. Adults are unable to protect themselves from these policies and practices, let alone protect children. In addition, there is a general feeling of helplessness, guilt, and negligence because they have not succeeded in being

54. Abdullah, Tayseer. (2016). Factors associated with the phenomenon of violence in Jerusalem schools. Retrieved in (19/12/2024), from: Click.

the protective shield for children and are even forced to practice oppression as the only means they have to protect children. For example, schools and institutions received threatening letters from the Israeli authorities. In addition, all schools were subjected to periodic inspections from the Ministry of Education, which included inspections of books, notebooks, curricula, electronic devices, etc.

Moreover, there is a tension between children's rights and the role of caregivers; on the one hand, a child has the right to freedom, to access the Internet, to access information, and to privacy, and on the other hand, adults must safeguard children's interests and protect them from danger,[55] which is carried out through inspecting, confiscating and monitoring children's phones. and being perceived by the children themselves as a restriction on their freedom and independence. This constitutes another infringement to children's rights. Indeed, this dilemma has emerged in all interviews, highlighting that children fight for their agency and social autonomy by circumventing the punitive means of parents and caregivers.

The third and final barrier is related to the digital divide between children and caregivers. Children enjoy highly advanced digital and technological capabilities compared to adults, which limits the caregivers' ability to guide children on the appropriate, beneficial, and safe use of technology. This gap is not only digital. The need to develop a common language and dialogue between adults and children, and between service providers and beneficiaries, was also highlighted during the interviews. A dialogue is necessary in stimulating cooperation between different social actors and their willingness to listen, learn, and develop.

## 5.5 Digital protection tools and means

Children's understanding of digital safety is based on two basic components. First, maintaining privacy of information and data, and second, protecting electronic devices and digital accounts. The range of digital protection means and mechanisms is wide: using strong passwords, not sharing photos, or clicking on any link that may expose the device to hacking. The first group of protection means simply require refraining from a certain act or behavior in the digital environment. According to the study, the most frequently used means are:

1. Females should refrain from posting and sharing photos with friends in the digital sphere. However, no one saw an urgent need for boys to refrain from doing so, because they are not affected by such actions.

55. United Nations. General comment No. 25. Ibid.

2. Refraining from posting, especially on political issues.
3. Refraining from making the account public. Some of the children manage two or more accounts for different uses.
4. Refraining from accepting a friend request or communicating with strangers in the digital sphere.
5. Refraining from turning on the geolocation feature.
6. Refraining from turning on the camera and microphone during gameplay.
7. Refraining from saving passwords in random places.
8. Using strong passwords.
9. Changing passwords periodically.
10. Refraining from sharing passwords with friends and peers.

The protective methods that require the child to take simple steps and actions actively are less commonly used. For example:

1. Using two-step verification.
2. Using multiple emails to avoid hacking all accounts at the same time.
3. Receiving notifications when the account is accessed from a new device or location (login alerts).
4. Using a temporary credit card for any transactions they make in the digital sphere, especially for gaming.
5. Filtering the Internet and websites.
6. Preferring the apps that they consider to be safer. Voices have emerged in the children's groups in favor of using Snapchat for the following reasons: “For example, if you talk to someone and he take photos [screenshots], you will be notifies that he took a screenshot...” “in Instagram, for example, you can see my followers, those who follow me, but on SnapChat no one can see them,” “for example, the conversation on SnapChat is not saved and no one can see your friends list, so you feel it is safer...”.
7. Eventually, all caregivers and most children agree that the most effective way to protect them from digital abuses and risks is through digital awareness and education, for children and parents alike.

### 5.5.1 Support networks when exposed to digital breaches:

The children shared that they were instructed by their schools to contact the Israeli Cyber Police and 105 Hotline (The Child Online Protection Bureau) when their digital rights were infringed. In addition, most children and their parents contact these parties when their sons and daughters are subjected to very serious digital attacks such as extortion,

identity theft, threats, posting offensive images, etc. This indicates the readiness of some children, schools, and parents to approach the Israeli authorities responsible for dealing with these attacks, contrary to the results of a study conducted by the 7amleh Center in 2020.[56] However, as a result of police disregard for their approaches, accompanied by feelings that the Israeli police are hostile to Palestinians, there have been some voices questioning the extent of the police's willingness in providing them with assistance. The alternative to the Israel Police is to turn to digital security specialists.

After the official authorities, children tend to resort to their families, which indicates that there is a new generation of parents in Jerusalem who practice a different parental relationship with their children, compared to previous generations characterized by authoritarianism. Particularly, females expressed that they prefer to turn to one of their older brothers or sisters for help, believing they will be less strict and more understanding than their parents, which is an indicator of the emergence of a new generation that chooses a path different from the usual path in which siblings pose a threat to the safety and freedom of their sisters, or simply because siblings are more capable of using technology than parents. This is also true when children choose to turn to their friends for help.

However, there were few voices of females who indicated that they did not feel safe to turn to their parents in case they were cyberattacked and prefer to turn to distant acquaintances or teachers. Some even objected turning to teachers because they often report the assault to parents. The vacuum of support systems available to females without worrying about the consequences of sharing the assaults has sometimes led them to think about turning to social media “influencers” who promote themselves as “digital security specialists,” without questioning the integrity of these individuals, or even thinking that sharing their story with them may open the door to another attack.

## 6. Conclusion

The current study discusses the experiences of Palestinian children in Jerusalem with digital safety when they encounter technology at home, school, and different cultural and educational settings. The paper attempts to reveal the most crucial factors shaping these children's experiences, and the main threats to the exercise of their rights and their digital childhood. The paper also explores the identities of the social actors who are partners in violating children’s rights, as well as the social actors who try to empower these rights.

56. Berekdar, Mohanad. Ibid.

One of the most important findings of the study is that children repeatedly affirm their independence, activeness, effectiveness and social and political agency in their use of methods of using technological devices and their digital practices, thus, becoming partners in the production and formation of their social environment.[57] The study reveals that Jerusalemite children navigate a wide web of restrictions and risks that threaten their autonomy and digital rights, with the following factors playing a central role in threatening children's digital safety:

1. Gender factor: using specific types and forms of digital violations based on gender identity, especially blackmail, threats to post offensive images, and identity theft, in which societal concepts and norms about “honor”, “female body”, “beauty standards”, and “submission” are employed as tools to threaten the safety, reputation and security of females. On the other hand, distorted perceptions of masculinity have played a role in the violence inflicted by males on young males and females in the digital world, including societal immunity from his immoral practices towards females, or even excessive violence against males.
2. Social and economic factors: Children are exposed to a wide range of societal control mechanisms over their digital and daily behaviors. This is a result of a deficient view of children in society that considers them social property, and because of the density of social networks and relations in it. The dire economic situation in Jerusalem also plays a role in extortion and financial fraud that children have been subjected to and committed themselves for financial gain. In addition, resource and funding constraints limit the ability of schools and institutions to provide children with better services, technological development, and digital safety education.
3. Factors related to the educational relationship between children-parents-teachers. The nature and form of the parental relationship plays a key role in children's digital safety. The more parents trust their children and are a haven for them, the less likely their children are to be harmed by digital assaults. The situation is more complicated in schools, as there is a fundamental imbalance in the educational relationship between teaching staff and students, which may increase the severity of digital violations, or even the intensity of reactions to these violations.
4. Political and security factors: Israeli forces and authorities play a different role in terms of violating children rights in different periods. It seems that the genocide in Gaza has put the Israeli forces at the top of the reasons that threat the safety and rights of Jerusalemite children. Jerusalemite children have never known how to live unmonitored. The ghost of constant monitoring hovers over their routine and daily experiences. Like the rest of Palestinian society, children have internalized self-censorship resulting in a narrower space for freedom of expression and political participation. The inspection of phones constitutes a total violation of their childhood and humanity.

57. Lee, Nick. Ibid.

Consequently, the level of digital security for children depends on different social spaces, the roles occupied by social actors, and the political and field changes and transformations. Therefore, there is a need to address the above factors radically and comprehensively, for children to regain even a small part of their amputated childhood, and their human and digital rights, as the protection of digital rights has become a condition for protecting children's human rights, and vice versa.

# 6. Recommendations

## States and Authorities:

- No temporary solutions will provide a remedy for the digital attacks on children on political grounds. Therefore, the only solution that can put an end to these attacks is to end occupation.
- Removing all military checkpoints and preventing intensified monitoring against civilians passing through them.
- Punishment of all individuals who had a role in unlawful phone inspections and child abuse.

## The international community:

- The international community should adapt the list of children's rights to include children in conflict zones and be more sensitive to their experiences and abuses.
- It is crucial that there be an authority capable of holding governments that engage in child abuse accountable.

## Tech companies:

- Given the increasing amount of inappropriate content that children are unintentionally exposed to on the Internet, technology companies should use predictive algorithms that analyze the user's age and gender to block all similar content when children use the Internet.
- Companies should refrain from banning, blocking, and restricting Palestinian content, especially when users are children.
- Tech companies should consider and respect the opinions and attitudes of children when updating their digital platforms, laws, and regulations, especially children affected by political marginalization. The testimonies in this study may be the beginning of this process.
- Tech companies need to take more stern actions on incitement and hate speech, especially those to which children may be exposed.

- Tech companies should include clear text about any additional update and provide children with the possibility of approving or rejecting it.
- Tech companies must provide effective mechanisms to verify the identity of users to reduce identity theft and ensure a safer digital environment.

## Funders:

- Funders are advised to develop a more holistic view of the intersection of organization works with digital security, and to integrate the digital security of organizations and child beneficiaries into their funding plans.
- Allocating funds for the development of the technical and technological aspects of institutions and encouraging the integration of technology in working methods.
- Funding social and digital projects for long-term periods to ensure the sustainability and financial stability of institutions.

## Child caregivers:

- To prevent children from committing digital abuses, there is a need to equip children with basic skills to manage their personal conflicts and control anger, emotions, and feelings.
- Caregivers should consider the child's autonomy and uniqueness when dealing with their digital behaviors and maintain an appropriate balance between the need to protect children and their other rights, including privacy.
- Promoting dialogue and communication between caregivers and children, service providers, individuals and beneficiaries, through tools of persuasion that push them to put digital safety on their agendas.
- It is essential to guide and direct children's evolving digital capabilities in a positive and beneficial direction that may benefit them and society.

## Civil society organizations:

- Given the unique legal status of children in Jerusalem, there is a need to develop a community-based initiative that is able to address attacks against children in Jerusalem independent of the Israeli authorities.
- Raising awareness and legal knowledge of digital rights for adults and children alike.
- Training employees in digital security, and enhancing the security of systems, computers, and electronic software in the institution.
- Equipping staff with initial tools to deal with digital abuses against children before turning to outside help.

- Strengthening cooperation and networking between the various institutions in Jerusalem and working together for the greater interest of protecting children's rights.
- Individuals undergoing training in digital security should take it upon themselves to pass this knowledge on to all employees of the organization.
- It is important to promote a holistic view among institutions that the digital safety of children already intersects with their areas of specialization and work, especially as the effects of digital violations are reflected in other aspects of children's lives: education, social, psychological, and cognitive.
- Developing internal protocols and policies around digital security, while ensuring that future plans include this topic.

## Schools and decision-makers in education:

- Schools should rethink how education is digitized. The transition to digitization must be gradual and in consultation with students and consider their experiences and attitudes.
- All schools must ensure that their electronic devices are updated and provided with basic protection.
- The Ministry of Education and all schools should take it upon themselves to train teachers in digital safety.
- Recruiting a Digital Safety Officer at the school and enhancing the response to Digital attacks within the school.
- Developing clear protocols and policies on the use of technology within the school for all actors.
- Working to fix the imbalance in the educational relationship between the teacher and the student.
- Including weekly classes to train children on digital security and developing computer study curricula to include this aspect as well.

## Parents and families of children:

- Parents should take responsibility and develop their technological and digital knowledge and skills.
- Parents should maintain a healthy relationship with their children based on affection, trust, and understanding. This safety net may be a last frontier in combating digital assaults.
- Parents should ensure that telecommunications companies provide them with filtered internet at home.

## Organizations that provide services in digital security:

- Developing workshops and training for all caregivers of children, such as parents, schools, and civil society institutions.
- Providing caregivers with mechanisms and tools to optimally pass this knowledge on to children.
- Developing joint interactive workshops and training on digital security for parents and children to enhance communication between them on technology use.
- Creating awareness campaigns based on real stories of abuses against children, discussing with children the best practices to deal with each case.
- Developing training on the beneficial use of technologies. Children's technological skills seem to be limited to specific uses, while the full potential of technology is not exploited.
- Develop entertaining and fun means through which children can acquire tools and skills to protect themselves digitally, such as developing a digital game or employing virtual reality technology.
- Conducting a series of lectures or awareness videos for children and parents, especially about the dangers of digital games and threats to children's digital security.

# List of sources

## Sources in Arabic:


- Abdullah, Tayseer. (2016). Factors associated with the phenomenon of violence in Jerusalem schools. Retrieved in (19/12/2024), from: Click.
- Abu Mualla, Saeed. (2024, August 28). Digital Safety among Palestinian Youth at Home: A Study on Threats and the Challenges in Light of the war on Gaza. 7amleh Center. Retrieved in (19/12/2024), from: Click.
- Abu Mualla, Saeed. (2024, August 28). Digital Safety among Palestinian Youth: A Study on Threats and Challenges in Light of War on Gaza (West Bank and Jerusalem). 7amleh Center. Retrieved in (19/12/2024), from: Click.
- Al Jazeera Net. (2024, February). On their International Day... Children in Jerusalem are tortured inside and outside prisons. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
- Al Jazeera Net. (2024, February). Poverty in Jerusalem... The circle is widening and there is no horizon to narrow it. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
- Al-Rajoub, Awad. (2024, February). 29 martyrs in Jerusalem, half of them children, since October 7th. Al Jazeera website. Retrieved on (19/12/2024), from: Click.
- Amnesty International. (ND). Children's rights. Retrieved (December 19, 2024) from: Click.
- Berekdar, Mohanad. (2020, September 29). Digital Safety Among Jerusalemite Children and Youth. 7amleh Center. Retrieved on (19/12/2024), from: Click.
- The United Nations. (ND). Convention on the Rights of the Child. Retrieved (19 December 2024) from: Click here.
- The United Nations. (ND). Convention on the Rights of the Child: General Comment No. 25 (2021) on the rights of the child in relation to the digital environment. Retrieved on (19 December 2024), from: Click.
- Wafa. (ND). Violence in schools. Wafa - Palestinian News and Info Agency. Retrieved in (December 24, 2024), from: Click.

## Resources in English


- Bhadra, Bula. (Editor). (2013). Readings in Indian Sociology: Sociology of Childhood and Youth. California: SAGE Puplications.
- Cloudflare. (n.d.). What is Swatting?. **Cloudflare Learning Center**. Retrieved in (December 24, 2024), from: Click.
- Conway, Adam. (2022, April 15). *Dangers of Kernel Level Anti Cheats*. XDA Developers. Retrieved in (December 24, 2024), from: Click.
- Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Retrieved in (19/12/2024), from: Click.
- Cruz, Brett; Turner, Gabe. (n.d.). What is Doxxing?. **Security.org**. Retrieved in (December 24, 2024), from: Click.
- Economic Commission for Latin America and the Caribbean (ECLAC). (n.d.). Document hosted in CEPAL's repository. Retrieved in (19/12/2024), from: Click.
- Feldman, Allen. (2002). "X–children and the militarisation of everyday life: comparative comments on the politics of youth, victimage and violence in transitional societies". *International Journal of Social Welfare*, 11(4), Pp. 286-299.
- International Telecommunication Union. (n.d.). Child Online Protection: Guidelines on Child Online Protection: Keeping Children Safe Online. Retrieved on (December 19, 2024), from: Click.
- Kaspersky. (n.d.). What is Adware?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
- Kaspersky. (n.d.). What is a Keylogger?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
- Kaspersky. (n.d.). What is Ransomware?. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
- Kaspersky. (n.d.). Top 10 ways to stop cyberbullying. **Kaspersky Resource Center**. Retrieved in (December 24, 2024), from: Click.
- Kaspersky. (n.d.). How to avoid cyberstalking. Kaspersky Resource Center. Retrieved in (December 24, 2024), from: Click.
- Kovner, Bella. (2020). "Children's rights, protection and access to justice: The case of Palestinian children in East Jerusalem". In: Roer-Strier, Dorit; Nadan, Yochay. (Edited). Context-informed perspectives of child risk and protection in Israel : Pp. 241-261.
- League of Legends Fandom. (n.d.). *Riot Vanguard*. **League of Legends Fandom**. Retrieved in (December 24, 2024), from: Click.
- Lee, Nick. (2013). "The extensions of childhood: Technologies, children and independence". In: Hutchby, Ian; Moran-Ellis, Jo. (Edited). *Children, Technology and Culture*. London: Routledge. Pp. 153-169

- Livingstone, Sonia; Blum-Ross, Alicia. (2017). "Researching children and childhood in the digital age". In: Christensen, Pia; James, Allsion. (Editors). *Research with children*. London: Routledge. Pp. 66-82.
- Livingstone, Sonia; Carr, John; Byrne, Jasmina. (2015). One in three: Internet governance and children's rights. Center for International Governance Innovation. Retrieved in (19/02/2024), from: Click.
- Oswell, David. (2013). "Ethics and techno-childhood". In: In: Hutchby, Ian; Moran-Ellis, Jo. (Edited). *Children, Technology and Culture*. London: Routledge. Pp. 170-183.
- PCGamingWiki. (n.d.). *Easy Anti-Cheat*. **PCGamingWiki**. Retrieved in (December 24, 2024), from: Click.
- Perekalin, Alex. (2020, April 3). *The dangers of cracked games*. **Kaspersky**. Retrieved in (December 24, 2024), from: Click.
- Shalhūb-Kīfūrkiyān, Nādirah. (2015). *Security theology, surveillance and the politics of fear*. Cambridge University Press.
- Shalhoub-Kevorkian, Nadera. (2019). Incarcerated childhood and the politics of unchilding. Cambridge University Press.
- Third, Amanda; Livingstone, Sonia; Lansdown, Gerison. (2019). "Recognizing children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice". In: Wagner, Ben; Kettemann, C. Matthias; Vieth, Kilian. (Edited). *Research handbook on human rights and digital technology*. Edward Elgar Publishing. 376-410.
- Wikipedia. (n.d.). *What is software cracking*. **Wikipedia**. Retrieved in (December 24, 2024), from: Click.
- Wikipedia. (n.d.). *BattleEye*. **Wikipedia**. Retrieved in (December 24, 2024), from: Click.
- Wired. (2023, July 17). Video games, data privacy, and artificial intelligence. **Wired**. Retrieved in (2024, December 24), from: Click.

Contact us:
info@7amleh.org | www.7amleh.org
Find us on social media: **7amleh**