Evidence-based Research on Palestinian Internet Access and Digital Rights

The Palestinian Initiative for the Promotion of Global Dialogue and Democracy “MIFTAH”

September 2024

Evidence-based Research on Palestinian Internet Access and Digital Rights

MIFTAH publications, 2024

Prepared by: Anderson Palestine

MIFTAH Team:

Khadeja Ibrahim	International Advocacy Officer
Abdalaziz Al-Salehi	Research and Studies Unit Officer

TABLE OF CONTENTS

1. Executive Summary

Digital rights are foundational to Palestinians' ability to exercise broader human rights, particularly in a context of occupation and conflict. Access to the internet enables education, communication, and advocacy, while the denial of these rights exacerbates social, political, and economic inequalities.

This report provides a comprehensive analysis of the state of digital rights in the Palestinian context, with a focus on violations perpetrated by both the Israeli occupation and the Palestinian National Authority (PNA). The research highlights how digital rights—encompassing the rights to freedom of expression, privacy, and access to information—are critical to the broader realization of human rights in the digital age. It examines the intersection of these rights with legal frameworks, technological advances, and socio-political dynamics in the occupied Palestinian territory.

Key Findings

Violations by the Israeli Occupation

- **Technological Oppression:** The Israeli occupation employs advanced technologies, including artificial intelligence, to target Palestinian civilians and suppress their digital rights. These measures are part of broader colonial and expansionist policies, constituting war crimes under international law.
- **Internet Disruptions:** Repeated and deliberate interruptions to telecommunications and internet services have been documented, particularly during military campaigns, with devastating impacts on civilian life, communication, and access to emergency services.
- **Censorship:** Social media platforms, often under pressure from the Israeli government, have removed or restricted thousands of posts related to Palestinian rights, silencing dissent and limiting freedom of expression.
- **Surveillance:** Pervasive monitoring and data interception are used to intimidate and control the Palestinian population, violating their right to privacy

Challenges within the Palestinian National Authority (PNA)

- **Limited Protection of Digital Rights:** The PNA lacks the capacity and political will to safeguard digital rights consistently, contributing to restrictions on freedom of expression and weak enforcement of privacy protections.
- **Internal Violations:** Reports indicate instances of censorship, surveillance, and intimidation by Palestinian authorities, targeting journalists, activists, and ordinary citizens.

2. Introduction

With the advancement of technology, Palestinian rights, like those of other peoples of the world, are practiced in both physical and digital spheres. 'Digital Rights' refers to those human rights exercised in the digital sphere, which include the rights to freedom of expression, privacy, and access information. These rights are largely dependent on internet access.

In the Palestinian context, those responsible for upholding these digital rights in Occupied Palestinian land are the Israeli Authorities and the Palestinian National Authority (PNA).

Israel's occupation of Palestine has been characterized from the start by violations of the basic rights of Palestinians. The magnitude of these violations has typically increased during times of active hostility. The Israeli occupation[1] uses modern and innovative methods to oppress Palestinians and crush their existence in order to achieve its colonial and expansionist aims, in contravention of international laws and norms – especially, international human rights law and international humanitarian law – as most of the occupation's colonial and settlement policies and practices constitute war crimes and crimes against humanity according to international criminal law. In its recent assault on the Gaza Strip that began in October 2023, the Israeli occupation has employed a range of technologies, including extensive use of artificial intelligence, to illegally target Palestinian civilians.

The Palestinian National Authority (PNA) has not demonstrated the capacity or will to ensure the digital rights of Palestinians consistently. This constitutes a violation of international human rights law, represented by the international treaties to which the PNA acceded in 2014.[2]

Palestinian women in particular are impacted by digital rights violations in gender specific ways. They face digital gender-based violence, societal and structural challenges which limit their freedom of expression online and are at the receiving end of smear campaigns and defamation.

This study reviews the most significant practices implemented by the Israeli occupation and the Palestinian Authority that violate digital rights and contravene international law and analyzes the domestic legal frameworks that are used by both parties to support and enhance their ability to violate these rights. Israel's use of technologies such as artificial intelligence to suppress digital rights as part of its current assault on Gaza is also explored. The study also addresses the role of private companies, specifically Palestinian telecommunications companies, in this matter.

[1] The term 'the Israeli occupation' or 'the occupation' is used throughout this document due to the fundamental nature of Israel as an entity occupying Palestine. Please see Amnesty report Israel's occupation: 50 years of Palestinian oppression - Amnesty International

[2]- Check the international agreements that the State of Palestine has joined: www.mofa.pna.ps

Spatial scale: Digital space, West Bank (including East Jerusalem), Gaza Strip.
Temporal scope: October 2023 - September 2024.

Significance: With rapid technological advances, digital rights have become an integral aspect of contemporary human rights, reflecting how individuals exercise their rights in the digital space. Palestinians have an urgent need to realize their digital rights in order to fully realize their rights to freedom of expression, privacy, and access to vital information. These rights are directly affected by the ability to access the Internet, which is the primary means of communication, education, and knowledge sharing. Given the Palestinian context, it is essential to highlight the ongoing violations practiced by various authorities, especially in times of war, where technology can be a tool of rescue and survival on the one hand or a tool to be exploited to achieve illegal military objectives on the other. Digital rights play a central role in the ability of Palestinians to present their own narrative, mobilize global support and solidarity, preserve their cultural identity and work toward self-determination.

Purpose: This study aims to provide a comprehensive analysis of digital rights violations in Palestine, focusing on the practices of both the Israeli occupation and the Palestinian National Authority. The study deconstructs the legal and social dimensions of these violations, exploring the use of modern technology such as artificial intelligence to enact policies of oppression, such as smear campaigns against human rights defenders, and the exploitation of societal gaps to exacerbate the effects of occupation and gender oppression. It also explores the domestic legal frameworks that play a role in these violations, contributing to a deeper understanding of how law intersects with the rights of individuals in the digital space. The study provides practical recommendations to strengthen the protection of Palestinians' digital rights and stimulate debate on the importance of these rights to promoting democracy and social justice.

3. Methodology and Limitations

This study relies on a descriptive-interpretive approach to revisit the violations that have occurred, describe them, and link them to the lived reality, analyzing the Palestinian context in light of the Israeli war on Palestinians. It includes an exploration of digital rights and access to the internet in the West Bank, Gaza Strip, and East Jerusalem, with a focus on Israeli violations against Palestinians and their digital rights.

The research began by identifying the main stakeholders involved, such as civil society organizations, government agencies, and international organizations, to facilitate the collection of necessary data in the data-gathering phase.

It is crucial to emphasize that ethical considerations are of particular importance, and it is essential to ensure respect for participants' rights through informed consent and the protection of confidentiality and participants' rights.

Regarding the data collection process, the primary data sources were international agreements, such as international humanitarian law, international human rights charters, human rights treaties, and recommendations and reports from international institutions and influential bodies to understand their impact on the Palestinian situation. This includes analyzing the legal frameworks implemented by Israel and the Palestinian Authority through a comprehensive legal review of international charters, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Additionally, the study's authors conducted a focus group with human rights defenders, youth influencers, activists, and civil society organizations working in the field of general rights, particularly digital rights.* The researchers also conducted a series of field interviews with representatives from Palestinian civil society organizations, official bodies, and private sector representatives, such as internet service providers, to gather insights into the reality of internet access and digital rights. An interview was conducted with telecom expert Magdy Hajj Khalil, in addition to an interview with Nader Al-Aloul, a representative of Mada Company. Furthermore, a series of individual interviews were held with professionals in the private sector, who requested that their names not be publicly listed as part of the respondents.

It is worth noting that preparing this study was not without challenges, as information regarding the use of technologies, including artificial intelligence, to violate privacy during the current assault on Gaza is very scarce, as most reports rely on inaccurate analyses due to the confidential nature of available intelligence information. The reluctance of many human rights defenders and representatives of the private sector to speak freely about these violations also reflects an environment of self-censorship resulting from the increasing threats they face. Although some official bodies have shown interest in this issue, the attention of the Palestinian Authority has been focused on other issues – particularly in the context of forming a new government – which has resulted in limited investment in the protection of digital rights. It is also worth noting that the private sector often avoids talking about issues related to human rights, due to the overlap of its interests with government approvals and permits. In addition, the size, number, and diversity of technical violations have complicated the documentation process, and many victims are reluctant to share their experiences for fear of consequences. Formal institutions, too, have indicated that the number of digital violations reported to them are not an accurate reflection of reality, due to the difficulty of documenting all cases.

The challenges can be summarized as follows:

1. Scarcity of technical and security information

Information regarding the technologies used during the current assault on Gaza, especially regarding AI-based tools and security techniques, is very scarce; most of this information is either not publicly available or is classified. The information that is circulated is mostly inaccurate analyses and estimates, making it extremely difficult to understand the full picture of technological violations. This poses a major challenge for any study that relies on accurate data to provide informed recommendations.

2. Self-censorship and refusal to testify

Human rights defenders and private sector representatives were reluctant to freely express their opinions about digital and real-world violations; self-censorship imposed by the nature of the violations, especially with regard to privacy and digital rights, prevented the study from obtaining direct and comprehensive information and testimonies. This limits the credibility of the data collected, as fear of legal and social consequences and repercussions remains an influential factor in restricting free disclosure.

3. Priorities of the Palestinian government

Despite officially stating an interest in digital rights, the Palestinian government, which was formed during the war, has faced political and internal issues that prevented it from giving sufficient attention to digital rights.

* On September 16th, 2024, several Palestinian civil society organizations concerned with human rights met to discuss developments in the Palestinian digital rights landscape from October 7th, 2023, to September 1st, 2024. The meeting was attended by the Arab Center for the Development of Community Media (7amleh), Human Rights Watch, Al-Haq Institute, the Independent Commission for Human Rights, the Jerusalem Legal Aid Center, and Miftah.

4. Reluctance of the private sector to engage with human rights

The private sector has generally avoided involvement in human rights issues, especially in light of its complex relationships with governments that grant it the licenses and permits necessary for its operations to continue. Companies operating in the digital sector tend to avoid criticizing government or engaging in human rights discourse for fear that their work will be obstructed or restricted.

5. Difficulty with documentation due to the wide scope of violations

The scale of digital violations, both geographically and numerically, has increased dramatically, making accurate documentation almost impossible. In addition, victims are reluctant to share their experiences due to fear of repercussions, whether from the occupation or from local authorities. Moreover, digital documentation itself has become more complex due to the increase in violations and the inability to keep up with the huge number of cases that require documentation.

4. Legal Context

The international instruments that govern human rights – primarily the Universal Declaration of Human Rights of 1948, the International Covenant on Civil and Political Rights of 1966, and the International Covenant on Economic, Social and Cultural Rights of 1966 – were drafted before the digital era and do not explicitly define the concept of digital rights. However, in the digital age, access to the Internet has become essential to individuals' ability to exercise their human rights. The United Nations General Assembly has recognized this in Resolution 68/167: "The same rights that people enjoy offline should also be protected online.[3] " The United Nations Human Rights Council – which adopted the Universal Declaration of Human Rights (UDHR) in 1948 and the International Covenant on Civil and Political Rights (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR) in 1966 – has also adopted several resolutions recognizing the importance of the Internet to the exercise of human rights. This includes Resolution 32/13 of 2016, which prohibits any measures aimed at preventing or disrupting access to information online[4].

Digital rights, as the exercise of human rights in virtual space, have become integral to the full enjoyment of the rights to freedom of expression, access to information, and privacy. Access to the Internet is thus essential to enable individuals to fully exercise these rights. The European Court of Human Rights has emphasized the importance of internet access for the exercise of fundamental human rights, particularly the right to freedom of expression[5].The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stated that access to the Internet is key to enabling this right[6].

Human Rights as Digital Rights

1. Right to Freedom of Expression

The right to freedom of expression is one of the fundamental rights guaranteed and protected by clear and explicit provisions under international human rights law. Article 19 of the Universal Declaration of Human Rights states: "Everyone has the right to freedom of opinion and expression. This right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This text also appears in the International Covenant on Civil and Political Rights (ICCPR), where Article 19 states that "Everyone has the right to hold opinions without interference and the right to freedom of expression.

[3] UNGA, Res 67/168. Paragraph 3.

[4] A/HRC/RES/32/13

[5] European Court of Human Rights: Case of Ahmet Yıldırım v. Turkey; European Court of Human Rights: Case of Cengiz and Others v. Turkey

[6] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

This right includes freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Paragraph (3) of the same article states that the exercise of these rights may be subject to certain restrictions for respect of the rights or reputations of others, or for the protection of national security or of public order, public health or morals, provided that these are prescribed by law and are necessary. Comment No. 34 of the Human Rights Committee, expressly protected opinions include political, scientific, historical, moral, ethical, and religious opinions; individuals have the freedom to change their opinions at any time.

Freedom of expression intersects with other rights and freedoms, such as the freedom to hold and express – or not to hold and express – opinions and the freedom of the press in all its forms, including the Internet and other modern means of communication. It is also linked to political freedoms such as the rights to vote and to peaceful assembly, and freedom of thought, conscience, and religious practice.

Restrictions on the right to freedom of expression and/or the right to access to information are limited to two specific situations stipulated in Article 19(3) of the International Covenant. First, the exercise of these rights may not infringe on the rights and reputations of others; second, it may not compromise national security, public order, public health or public morality. Any restrictions must be aimed at protecting a legitimate and compelling public interest and must meet the following criteria:

- Legality. There must be a clear and available legal framework that precisely defines the situations in which restrictions can be imposed, which must not contradict the essence of Article 19 of the ICCPR and its general principles.
- Necessity. Restrictions must be essential and urgent to safeguard legitimate public interests.
- Proportionality. There must be a clear link between the restrictions and the interest for which they are imposed, and the restrictions must be within the limits necessary to preserve that interest.[7]

In the digital context, examples of state violations of the right to expression include blocking websites that oppose government policies, entering into agreements with social media administrations to close pages or delete posts and prevent the publication of certain materials, and criminalizing the use of social media to criticize government policies.

2. Right to Privacy

The right to privacy is one of the fundamental rights articulated explicitly in international human rights law. Article 12 of the Universal Declaration of Human Rights states:

No one shall be subjected to **arbitrary [or unlawful] interference** with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The same statement is found in Article 17 of the International Covenant on Civil and Political Rights.

Principles of legal intervention to restrict the right to privacy[8]

To ensure that interventions that restrict the right to privacy are legal and are not arbitrary, authorities must comply with four key principles: legality, proportionality, necessity, and authorization by an independent and impartial judicial body.

[7] UN Human Rights Committee (HRC), General comment no. 34, Article 19, Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, bit.ly/3Nry7z7, accessed 24 August 2024.
[8] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://bit.ly/4dIGReP, accessed 24 August 2024,

Legality specifies that any interference with the right to privacy must have a clear and specific legal basis that complies with the provisions of the International Covenant on Civil and Political Rights: this requires an explicit legal text that defines the conditions of the intervention and places it within a recognized legal framework, to avoid any overreach by the authorities.

Proportionality requires that the intervention be proportionate to the goal it seeks to achieve, so that there is a logical and strong link between the intervention and the desired goal. The intervention must be justifiably necessary to achieve the objective, without being excessive or unjustified compared to the expected outcome.

Necessity stipulates that the intervention must be essential and urgent to achieve a legitimate goal. This mandates that the intervention must be the only means of achieving the desired objective and that it must be necessary at the present time, with no other less effective alternatives available.

In the context of proportionality and necessity, the legitimate aims of the law **include uncovering the circumstances of a particular crime, fighting crime, and maintaining national security.** These objectives require the aims to be defined, clear, and accessible according to a layperson's standard, and there must be a specific case justifying the interference, where the legality, necessity, and proportionality of the interference are evaluated on a case-by-case basis.

The requirement for **authorization by an independent and impartial judicial body** mandates that any interference with the right to privacy be authorized by an independent judiciary that is not subject to outside influences. This requirement aims to protect individuals from the abuse of executive powers and ensures that authorization is based on an objective and independent assessment of the legitimacy and necessity of interference. Any interference with the right to privacy requires judicial authorization issued by an independent judicial body that is not subject to external influences. This authorization must include the specific details of the persons involved, the purpose of the interference, the information expected, and the timeframe of the intervention.

In the context of digital rights, examples of abusive government interventions include the use of blanket surveillance systems without a clear legal framework and collaboration with third parties such as telecom companies, internet service providers, and social media sites to store personal data for later use. These interventions are characterized by the absence of a clear legal basis or adequate protection for individuals.

3. Right to Access Information

The right to access information is one of the basic rights that promote democracy, transparency, and accountability in a political system. It is recognized as a human right and a digital right in the International Covenant on Civil and Political Rights (ICCPR) and other international conventions. Article 19 of the ICCPR stipulates that “everyone shall have the right to hold opinions without interference, and shall have the right to seek, receive and impart information and ideas of all kinds in any form of expression.” This highlights the importance of access to information as a tool to achieve freedom of expression and ensure transparency.

The General Comments issued by the Human Rights Committee interpret this right broadly. General Comment No. 34 (2011) states: “The right to access information held by public authorities is an integral part of the right to freedom of expression.” This right includes the right to information about public matters that affect the lives of individuals and society. The General Comment also emphasizes that the right to access information enhances the ability to exercise other rights such as freedom of expression and participation in public affairs.

In the digital age, access to digital information has become a fundamental right to ensure freedom of expression and communication online. The United Nations Declaration on the Right to Access Digital Information recognizes that “access to digital information is essential for the exercise of fundamental rights and freedoms in the digital environment.”

These principles are also in line with international resolutions that emphasize the need to protect the right to access information as part of human rights in cyberspace, and to ensure that access to information on the Internet is not unduly restricted.

Given these provisions and comments, the right of access to information is an essential part of civil and political rights, and states must ensure that this right is protected and promoted in line with international standards to ensure freedom of expression and effective participation in public affairs.

The **right to access information** is usually linked to the right to education, which is a basic human right. This includes e-learning, which involves interactions in the digital space and is considered part of the digital rights that focus on ensuring individuals have access to digital competencies, technologies and resources as part of achieving quality and inclusive education.

The definition of the digital right to education indicates that the right to education as a digital right is an extension of the traditional right to education, as it includes access to digital education resources such as the Internet, online educational platforms, and educational software. This dimension ensures that all individuals have the ability to utilize modern technologies as part of their educational experience.

International law that speaks to the right to education, such as the Universal Declaration of Human Rights – which, in Article 26, states that ‘‘everyone has the right to education’’, are now interpreted to include e-learning. Similarly, the International Covenant on Economic, Social and Cultural Rights (ICESCR), which emphasizes in Article 13 that education should be available and accessible to all, is now interpreted with the understanding that digital technology must be made available as a means of education. General Comment No. 13 (1999) of the Committee on Economic, Social and Cultural Rights emphasizes the importance of education being **‘‘adaptable’’**; this is now understood to include digital literacy and access to digital resources as part of the right to education. **General Comment No. 25 of 2021** highlights the need to integrate digital inclusion into the right to education and ensure that digital technology is fairly and equitably accessible to all individuals.

4. Access to the Internet

The Office of the United Nations High Commissioner for Human Rights defines internet shutdown as follows:

“All measures undertaken by the government or on its behalf that intentionally prevent or disrupt access to, or dissemination of, information online are shutdowns. Shutdowns come in a wide range of forms, including bandwidth throttling to slow internet access, blocking of specific apps that are essential for interactive communications, such as social media or messaging services”[9].

[9] Internet shutdowns: Trends, causes, legal implications and impacts on a range of human rights. Report of the Office of the United Nations High Commissioner for Human Rights, 13 May 2022, A/HRC/50/55, Paras 4-6, https://bit.ly/404DPP2

This definition highlights that it is not only a complete shutdown of internet connectivity or access to services that qualifies as a shutdown. Governments are increasingly resorting to throttling bandwidth or reducing mobile service to 2G, making it extremely difficult to use the Internet to watch or share videos or to livestream. Similar interventions also reduce the availability of services to prevent people from circumventing shutdown measures.

The OHCHR states that “[a]s technology evolves, so will the ways in which access to and use of cyberspace are disrupted, requiring changes in the definition of shutdowns and responses to them,” and stressed that knowledge of the intention of state actors to block access to the Internet is crucial to determining whether a shutdown is intentional and not the result of a technical error. An Internet shutdown does not refer to a loss of service as the result of technical issues with national infrastructure but, rather, indicate a voluntary act by a state to block the digital environment. Other deliberate actions by authorities that result in restricted functionality of infrastructure, such as the shutdown of energy or telecommunications services, may carry similar bad faith connotations and negative effects[10].

A 2015 Joint Declaration by experts on freedom of expression representing the United Nations, the Organization for Security and Co-operation in Europe, the Organization of American States and the African Commission on Human and Peoples’ Rights reaffirmed the illegality of internet shutdowns by stating that “filtering online content, using ‘kill switches’ (i.e. shutting down entire parts of communications systems) [...] are measures that can never be justified under human rights law".[11]

Former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, also stressed that internet shutdowns are “generally disproportionate”, and said that “even if they are based on national security or public order, they often tend to prevent the communications of millions of individuals[12].”

A report by the Office of the United Nations High Commissioner for Human Rights states that “internet shutdowns are strong signs of deteriorating human rights conditions.” It noted that in situations of armed conflict, “the inability to access the tools needed to document and report violations quickly contributes to the escalation of violence, including atrocities. Some shutdowns may also be carried out deliberately to cover up human rights violations.” Given the indiscriminate scale and wide-ranging negative impacts of internet shutdowns on many rights outside the areas or periods in which they are implemented, the report stresses that these operations “rarely meet the basic requirements of necessity and proportionality, making them disproportionate, even when intended to respond to real threats".[13]

[10] Ibid.

[11] The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. Document name missing. para. 4(c), available at: https://bit.ly/4h0D1AF. 4 May 2015. The 2011 and2015 Joint Declarations were reconfirmed in the Joint Declaration in 2016 and 2018. Further, the 2019 and 2020 Joint Declaration deplored specifically internet shutdowns and required that “[o]ver the coming years, States and other actors should […] [r]efrain from imposing Internet or telecommunications network disruptions and shutdowns.” For the 2020 Joint Declaration, see: https://bit.ly/3Y7yaF0

[12] UN General Assembly.Report of the Special Rapporteur on the Promotionand Protection of the Right to Freedomof Opinion and Expression, UN Doc.A/71/373, para.21, available at: https://undocs.org/en/A/71/373, 6 September 2016.

[13] UN General Assembly. Report of the Office of the UnitedNations High Commissioner for Human Rights on Internet shutdowns: Trends, causes, legal implications and impacts on a range of human rights, UN Doc. A/HRC/50/55, available at: https://bit.ly/3A9c4dg 13 May 2022.

The 2016 UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the Internet, adopted unanimously, also unequivocally condemns measures aimed at deliberately preventing or disrupting access to, or dissemination of, information online, which constitutes a violation of international human rights law. It also calls on all states to refrain from and cease any restrictive measures. [14]

In May 2020, the Secretary-General of the United Nations stressed that “blanket internet shutdowns, blocking and general filtering of services constitute a violation of international human rights law.”[15].

In December 2023, the UN General Assembly, in its resolution on the promotion and protection of human rights in the context of digital technologies, reaffirmed the obligation of states to protect human rights and fundamental freedoms, both online and offline. It unequivocally condemned “the use of blanket Internet shutdowns and unlawful restrictions to intentionally prevent or disrupt access to or dissemination of information online,” and stressed the importance of a free, open, interoperable, reliable and secure Internet.

The UN Charter on Human Rights and Principles of the Internet recognizes the following principles with respect to human rights realized through the Internet:[16]

1. **Universality and Equality:** All humans are born free and equal in dignity and rights, which must be respected, protected, and fulfilled in the online environment.
2. **Rights and Social Justice:** The Internet is a space for the promotion, protection and fulfillment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.
3. **Accessibility:** Everyone has an equal right to access and use a secure and open Internet.
4. **Expression and Association:** Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.
5. **Privacy and Data Protection:** Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.
6. **Life, liberty and security:** The right to life, liberty and security on the Internet must be respected, protected and fulfilled. These rights must not be infringed upon, or used to infringe other rights, in the online environment.
7. **Diversity:** Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.
8. **Network Equality:** Everyone shall have universal and open access to the Internet’s content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds.
9. **Standards and Regulation:** The Internet’s architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.
10. **Governance:** Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability.

---

[14] UN Human Rights Council Resolution (A/HRC/RES/32/13) on the Promotion, Protection, and Enjoyment of Human Rights on the Internet. This was the first UN resolution that spoke directly to internet shutdowns. This language has been repeated and strengthened in various resolutions since 2016.

[15]UN General Assembly. Road map for digital cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation, UN Doc. A/74/821, para. 41, available at: https://undocs.org/A/74/821, May 29, 2020

[16]Internet Rights & Principles Coalition, The charter of human rights and principles for the internet - United Nations https://bit.ly/3U9wn17

Legal Framework Governing Digital Human Rights in the Palestinian Context

Internet access is essential in times of both peace and war because it enables people to communicate, exchange information, and express their opinions freely. In times of peace, the Internet promotes civic engagement and enables individuals to access education, health services, and vital information. In times of conflict, the Internet plays a vital role in disseminating news, coordinating humanitarian responses, and safeguarding human rights as it facilitates the exercise of other rights, including freedom of expression and assembly. Internet access enables an active civic space, thus strengthening democracy and promoting accountability. The Internet thus plays an essential role in protecting and promoting civil rights in all circumstances. A review of the regulatory frameworks applicable in the Occupied Palestinian Territories (Gaza Strip and the West Bank, including East Jerusalem) shows that international human rights law (IHRL) and international humanitarian law (IHL) mandate specific legal obligations for those bodies responsible for the respect and protection of these rights ("duty bearers"), as detailed below.

1.Israel (Occupying Power)

- **International Humanitarian Law**

International humanitarian law (IHL) imposes clear obligations on occupying powers, even in the absence of active hostilities. These include safeguarding basic human rights such as freedom of expression, the right to privacy, access to information, and the right to education. The Fourth Geneva Convention of 1949, particularly Article 47, obliges occupying powers to treat the population under occupation humanely and to respect their existing rights. Similarly, Article 43 of the Hague Regulations of 1907 requires the occupying power to restore public order and safety while respecting the laws in force in the occupied territory.

The International Court of Justice (ICJ), in its 2004 Advisory Opinion on the Legal Consequences of the Construction of the Wall in the Occupied Palestinian Territory, affirmed that Israeli-imposed measures must comply with both international human rights and humanitarian law, including digital rights. These protections are reinforced by the International Covenant on Civil and Political Rights (ICCPR), particularly Articles 17 and 19, which safeguard the rights to privacy and freedom of expression, and to access information.

Digital rights, including access to digital education, are part of Israel's obligations as an occupying power. General Comment No. 13 (1999) by the Committee on Economic, Social, and Cultural Rights defines education as needing to be "adaptable," which includes digital literacy and access to digital resources. General Comment No. 25 (2021) further stresses that digital inclusion must be part of the right to education and that digital technology must be accessible to all equitably.

Israel, as a party to the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR), and bound by the core provisions of the Geneva Conventions, is obligated to protect the civilian population in the territories it occupies. Articles 25, 27, and 47 of the Fourth Geneva Convention require the preservation of civilian rights and dignity, including access to communication, protection from violence, and the continuation of local laws and rights during occupation.

Accordingly, Israel is required to ensure internet access for Palestinians in both times of peace and during hostilities. Its failure to enable the Palestinian telecommunications sector—by denying licenses, obstructing the construction of infrastructure, especially in Area C, and restricting access to advanced technologies—violates these obligations. The deliberate cutting off of electricity and fuel, resulting in the collapse of communication services, as well as repeated internet shutdowns during military campaigns, further intensify civilian suffering and impede access to vital information and humanitarian aid.

Such actions not only hinder the population's ability to exercise fundamental rights but can also be used to conceal human rights violations and crimes under international law. The weaponization of internet access by Israeli authorities—through censorship, collective punishment, and disruption of vital services—has profound psychological, physical, and economic effects on civilians in Gaza and the West Bank.

These are not isolated incidents but rather part of a systematic policy aimed at repressing Palestinians' digital and civil rights. This includes the targeting of telecommunications infrastructure, the blocking of modern technology, and the killing of communications workers. Collectively, these practices constitute violations of international human rights and humanitarian law and may amount to war crimes and crimes against humanity. They are also part of a broader regime of racial discrimination and control imposed on the Palestinian people.

- **International Human Rights Law**

The obligation of Israel as the occupying authority to protect and respect human rights in the OPT arises from the effective authority it exercises as an occupying state, such that a state's obligation under international human rights law extends beyond its territorial boundaries to include areas it controls, albeit outside the sovereign territory of that state.[17]

"Israel -as an occupying power, has refused to implement its obligations under international law beyond the borders of its national territory[18]. The Israeli occupation authorities' failure to fulfill their human rights obligations in the Occupied Palestinian Territory (the Gaza Strip and the West Bank, including East Jerusalem) is reflected in relevant General Assembly resolutions[19], reports of the Secretary-General[20], reports of the United Nations High Commissioner for Human Rights[21], and various human rights treaty bodies[22].

In 2004, the International Court of Justice (ICJ) confirmed that Israel, as an occupying power, has obligations with regard to the Palestinian population[23]. The Court also noted that Israel's obligations under the International Covenant on Economic, Social and Cultural Rights include not creating obstacles to the exercise of these rights in areas where jurisdiction has been transferred to the Palestinian authorities[24]. It noted that the accession of the State of Palestine to human rights treaties does not affect Israel's human rights obligations in the OPT[25].

As a party to the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), Israel is obligated to respect and protect the fundamental human rights enshrined in these instruments of people living under its effective control, including digital rights such as freedom of expression, access to information, privacy, and education. In the digital age, access to the Internet is an integral part of these rights, enabling individuals to exercise their freedom of expression, access information, and communicate with the outside world.

[17] See: Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 134, para. 109.

[18] See, for example: E/C.12/1/Add.27, para. 8. See also Legal Consequences of the Construction of a Wall, para. 112.

[19] See, for example: General Assembly Resolution 98/71.

[20] See: A/69/348, paragraph 5, and A/HRC/28/44, paragraph 6.

[21] See, for example: A/HRC/8/17, paragraph 7, and A/HRC/12/37, paragraphs 5 and 6.

[22] See: Human Rights Committee general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the International Covenant on Civil and Political Rights, paragraph 10. See also: 90 E/C.12/1/Add.31; 4/CCPR/C/ISR/CO, paragraph 5; 2-4/CRC/C/ISR/CO, paragraph; 4/CAT/C/ISR/CO, paragraph 11; and CERD/C/IRS/CO/14-16, paragraph 10.

[23] See: Legal Consequences of the Construction of the Wall, paragraphs 110-113.

[24] Ibid, paragraph 112.

[25] See: A/AHRC/28/44, paragraph 6.

Denying Palestinians access to the Internet not only violates their rights to freedom of expression and access to information under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), but also undermines their right to education as stated in Article 13 of the International Covenant on Economic, Social and Cultural Rights (ICESCR). Access to online educational resources is critical to individual and community development and blocking access to these resources limits Palestinians' ability to develop their skills and access education. Under the Oslo Accords, the 1995 Interim Agreement on the West Bank and Gaza Strip (Oslo II) divided the West Bank into three areas (Areas A, B and C) with different responsibilities allocated to the PA and to Israel in each area. Although the PA has civil authority in Areas A and B, Israel retains full security control over Area C – which encompasses about 60 percent of the West Bank – and retains control over many vital aspects of infrastructure, including communications.

The provisions of Article 36 of the Oslo II Agreement, which addressed the issue of telecommunications and postal services, stipulated that: "Israel will continue to manage international communications, including satellite, shortwave, and short-range communications." This means that the Israeli occupation authorities retain significant control over the telecommunications infrastructure in the Palestinian territories. Since they effectively control this infrastructure, they are obligated to ensure that people living in the OPT, especially in Area C, have full and unrestricted access to the Internet as part of their digital rights.

Moreover, Article 40 of the Oslo II Agreement stipulates that both parties should cooperate in civil matters, which includes cooperation in the field of ICT. However, the restrictions imposed by the Israeli occupation authorities on internet access in the OPT contradict the spirit of this cooperation and constitute a violation of the obligations set forth in the Oslo Accords.

In light of the Israeli occupation authorities' obligations under the ICCPR and ICESCR, as well as in accordance with the responsibilities outlined in the Oslo Accords, Israel is required to ensure full access to the Internet and protect the digital rights of people living under its de facto control in the OPT. Any restrictions or violations of these rights could constitute a breach of international law and the agreed framework of the Oslo Accords.

- **Israeli Law**

First: The Illegality of Applying Israeli Law in East Jerusalem

The Israeli occupation engages in numerous practices, including applying its domestic law in East Jerusalem, that constitute a flagrant violation of international humanitarian law and represent a step toward de facto illegal annexation of the area. This contradiction is clear in the legal provisions and international resolutions that define the limits of an occupying authority and the protection to be afforded occupied territories.

Article 43 of the Hague Regulations on the Laws and Customs of War on Land of 1907 indicates that the occupying power is responsible for maintaining law and order in the occupied territory, but that: this must be done in conformity with the local laws of the territory.

The authority of the legitimate power having in fact passed into the hands of the occupant, the latter shall take all the measures in his power to restore, and ensure, as far as possible, public order and safety, while respecting, unless absolutely prevented, the laws in force in the country[26].

[26] https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907/regulations-art-43

International humanitarian law stipulates that an occupying power cannot impose its domestic law on the local population of an occupied territory. The application of Israeli law in East Jerusalem violates this principle: the legal and administrative regime of the occupied territory is being unlawfully altered, contradicting the basic principles enshrined in the Hague Regulations.

Moreover, UN Security Council Resolution 242 of 1967 calls for the withdrawal of the Israeli occupation authorities from the territories they occupied during the 1967 war, including East Jerusalem. This resolution proves that the de facto annexation of East Jerusalem is illegal and emphasizes that Palestinian sovereignty must be respected that the status quo may not be changed. The imposition of Israel's domestic law in East Jerusalem violates these principles and reinforces the de facto annexation of the area, which is contrary to UN Security Council Resolution 242.

UN Security Council Resolution 338 of 1973 reaffirms Resolution 242 and emphasizes that Israel is required to withdraw from the occupied territories; the resolution thus reinforces the opposition of the international community to any unilateral measures, including the imposition of domestic law in occupied territories. In summary, the application of Israeli law in East Jerusalem violates international resolutions and reinforces Israel's illegal de facto annexation of East Jerusalem in violation of international legal principles.

In addition, the 2004 advisory opinion of the International Court of Justice (ICJ) confirms that the construction of the Separation Barrier in the West Bank, including East Jerusalem, constitutes a violation of international law. Although the opinion focuses on the Wall, it highlights that the imposition of domestic law by an occupying power is a violation of the laws of occupation; thus, the imposition of Israeli law in East Jerusalem represents part of a policy of unlawful de facto annexation and constitutes an infringement on the rights of the local population.

Thus, the application of Israeli law in East Jerusalem constitutes a flagrant violation of international humanitarian law as enshrined in the Hague Regulations, Security Council resolutions, and the opinion of the International Court of Justice, which mandate that an occupying power has no right to impose its own domestic law on the local population of a territory that it occupies. As these practices contradict the basic principles governing the relationship between an occupying authority and the territory it occupies to ensure its protection and serve as part of a policy of illegal de facto annexation, they are illegal under international law.

Second: Israeli Law Regarding Digital Rights

- **The Right to the Freedom of Expression**

a. Basic Law: Human Dignity and Liberty of 1992. This is the foundational legislation that regulates human rights in Israel. Although it does not explicitly prescribe freedom of expression, the right to human dignity is often interpreted by courts to include the freedom of expression as part of the broader right to personal independence. This law is used as a legal basis for judicial decisions related to the protection or restriction of freedom of expression, especially when balanced against other rights.

b. The Defamation Act of 1965. This law places clear limits on freedom of expression by defining what constitutes defamation. Article 1 of the law states:

Defamation is something whose publication may –
(1) humiliate a person or make him or her an object of hatred, contempt or ridicule.
(2) Defame the reputation of a person because of acts, behavior or qualities attributed to him or her.
(3) Harm a person in his or her position, whether a public or other position, in his or her work or profession.
(4) Insult a person because of their race, origin, religion, place of residence, age, gender, sexual orientation, or disability; including civil and criminal liabilities related to speech that may harm an individual's reputation.

Article 6 of the law stipulates:
Whoever publishes defamation with the intention of harming two or more persons other than the victim shall be punished by one year imprisonment."

Article 7 states:
The publication of defamation of one or more persons other than the victim shall be considered a civil damage, and subject to the provisions of this law, the provisions of Articles 2(2) to 15, 55b, 58 to 61, and 63 to 68a of the Civil Torts Law shall apply. The 1944 Decree shall apply.

Threats of defamation lawsuits can create a chilling effect on freedom of expression, especially in the field of journalism and public criticism.

c. The Anti-Terrorism Order of 1948. This law bans any expression that supports or incites terrorism, including speeches, publications, and other forms of communication; it also includes a broad definition of terrorism that may lead to restrictions on political expression, especially in sensitive contexts such as the Israeli Palestinian conflict. Article 24 of the 2016 Anti-Terrorism Law states:

(a) Anyone who commits an act of identification with a terrorist organization, including publishing words of praise, support, or sympathy, waving a flag, displaying or publishing a symbol, or displaying, playing, or publishing a slogan or anthem.
(b) Whoever commits any of these acts shall be liable to a penalty of five years' imprisonment:

1. Publishes a direct invitation to commit a terrorist act.
2. Publishes words of praise, sympathy, encouragement, support or identification with a terrorist act and, depending on the content of the publication and the circumstances in which it was published, there is a real possibility that it could lead to a terrorist act."

It is worth mentioning that the law itself (Anti-Terrorism Order 1948) clarifies the meaning of words "publication or published" according to the 1977 Penal Code:

Article 34 K.D. "Publication" - writing, printed matter, computerized material or any other visual presentation, as well as any audio medium that may convey words or ideas, whether alone or with the aid of some means.

d. Censorship laws: The Israeli occupation authorities allow military censorship for the purpose of national security. Agreements between the government and the media set guidelines on what can be published; in the same vein, military censorship can limit the scope of public debate on security and defense issues. The first judicial ruling that tested the limits of freedom of expression in Israel when it conflicts with state security and public peace, is known as the Supreme Court's 'Voice of the People' ruling. In a long and reasoned judgment (HCJ 73/53), it established freedom of expression as a fundamental right and the supreme right under Israeli constitutional law, thus establishing for its successors the way in which civil rights and freedom of expression can be protected when they conflict with other competing interests. In the ruling, the "imminent certainty standard" was established, according to which freedom of expression will be withdrawn only when there is a near certainty of actual and serious harm to state security.

Article 9 of the Freedom of Information Act 1998 states that the state has the right not to provide certain information to the public and is obligated to do so in certain cases:

(a) A public authority may not provide information that is one of the following:

(1) Information the disclosure of which would be likely to prejudice the security of the State, its foreign relations, public safety or the security or welfare of a person.
(2) Information on issues determined by the Minister of Defense for reasons of maintaining the security of the State by decree with the approval of the Joint Commission.
(3) Information the disclosure of which would constitute an invasion of privacy, as defined in the Privacy Protection Act of 1981 (hereinafter - the Privacy Protection Act), unless disclosure is authorized by law.

e. The Anti-Boycott Law of 2011. This law penalizes publicly advocating for a boycott of Israel or its settlements, directly restricting certain forms of political expression. It also affects freedom of expression by deterring individuals or organizations from engaging in advocacy for boycott, sanctions, or divestment (BDS) for fear of legal consequences. Article 2 of the law states:

a) Anyone who knowingly publishes a public call to boycott the State of Israel, and according to the content of the call and the circumstances in which it was published, there is a reasonable possibility that the call will lead to an actual boycott, and the advertiser is aware of the said possibility, is civilly liable and will be subject to the provisions of the Torts Law [….] c) If the court finds that a tort under this Law was committed intentionally, it may order the tortfeasor to pay damages that are not dependent on the tort (deterrent damages); in determining the amount of damages, for example, the court will take into account, among other things, the circumstances, gravity and scope of the plaintiff's performance.

f. The Nakba Law of 2011. This law authorizes the Minister of Finance to reduce government funding to organizations that commemorate Nakba Day, the Palestinian day of mourning for the creation of Israel. By penalizing institutions that express certain views of history, this law restricts freedom of expression related to historical and cultural issues. Amendment No. 40 to the law states:

If the Minister of Finance considers that an organization has made an expenditure that is in essence one of those listed below (in this section - unsubsidized expenditures), he may, with the approval of the Minister in charge of the Budget Division, reduce the amounts to be transferred from the state budget to that organization in accordance with any law:

(1) Denying the existence of the State of Israel as a Jewish and democratic state.
(2) Incitement to racism, violence or terrorism.
(3) Supporting the armed struggle or terrorist action of an enemy state or terrorist organization against the State of Israel
(4) Considering “the Independence Day” or the “State Creation Day” a day of mourning.

g. The Entry into Israel Law of 1952. This law primarily regulates the entry of individuals into the country; however, it is also used to deny entry to people based on their expressed views, especially those perceived to support the boycott, divestment, and sanctions (BDS) movement or other forms of protest against Israel. Article 2 of the law states:
D. A visa and residence permit of any kind will not be granted to a person who is not an Israeli citizen or has a permanent residence permit in the State of Israel, if he or the organization or body in which he or she works, intentionally publishes a public call to boycott the State of Israel, as defined in the Prevention of Damage to the State of Israel through Boycott Law, 2011, or pledges to participate in such a boycott.

h. Israeli Penal Code of 1977. This law comprises several articles that regulate discourse, including incitement to violence and munity, abuse of religion, and incitement to racism. These provisions have a direct and indirect effect on the scope of permissible discourse. Article 173 states:

Any person who performs such an act shall be sentenced to an imprisonment of one year:

(1) Publishes a publication that intends to seriously harm the religious beliefs or feelings of others.
(2) Utters in a public place and in the hearing of a particular person a word or sound with the intention of seriously harming his or her religious beliefs or feelings.

i. Transparency Act 2021. This law aims to promote transparency in how social media platforms handle content moderation and user data. It requires platforms to disclose content moderation policies and procedures and includes provisions for appeals and grievances. Article 7 states:

Reports and notifications submitted by an association to the Registrar in accordance with the Act and these Regulations, including documents attached thereto under the Act, shall be open for review by any applicant, at the office of the Registrar, upon request, provided that no information prohibited by any law from being disclosed shall be published. (B) The Registrar may publish on the Internet, directly or via others, the reports submitted by the Society to the Registrar in accordance with the Law and these Regulations, including the documents attached thereto, the details contained therein, or part thereof, provided that no information whose disclosure is prohibited by any law shall be published.

j. The Anti-Incitement Act of 2014. This law focuses on combating incitement to violence or terrorism, whether online or through other media, and provides the legal basis for prosecuting individuals who publish content that incites violence or terrorism.

k. The Counterterrorism Act of 2016. This law expands the legal framework for counterterrorism; it including provisions related to online content and gives authorities the power to order the removal of content that supports terrorist activities and makes provision for penalties for non-compliance.

l. Cybersecurity Act of 2015. This law focuses on protecting national infrastructure against cyber threats, and includes provisions related to cyber threat management. It addresses the protection of digital assets and networks and includes requirements for reporting and remediation of cyber incidents, which can affect content management practices. Article 6 states:

(a) Information obtained from a supplier under this Act shall be kept confidential, shall not disclose it to others, and may only be utilized for the detection, prevention or containment of a serious cyber attack.
(b) Information received from the Supplier under this Act will be deleted immediately upon completion of the remediation of the serious cyber-attack, unless an eligible manager determines that the above information is necessary to characterize the cyber-attack; the information identified as described above will be retained to the minimum extent required.
(c) The public release of the plural form of a supplier's identity under this Act shall be with the approval of an eligible administrator after the supplier has had an opportunity to express its claims.

m. Draft Social Network Content Removal Act of 2018 (Facebook Act). Officially known as the Social Network Content Removal Act, this law aims to combat incitement to violence and terrorism online. The law allows authorities to request the removal of content deemed to incite violence or terrorism and makes provision for court orders to remove prohibited content from social media platforms such as Facebook and Twitter at the request of the authorities. It also provides a broad definition of what constitutes incitement, which raises concerns about how it could impact freedom of expression. In addition, the law imposes fines on platforms that fail to comply with court orders. (This law is still in draft form and has not yet been passed.)

n. Digital Platforms Bill 2020. This proposal aims to regulate digital platforms and their responsibilities in managing user-generated content. It includes provisions on content monitoring and removal and requires platforms to take proactive action against harmful content, with a focus on user safety and content management.

o. Administrative detention: Authorizes detention without trial of individuals based on their expressions or affiliations, especially in security cases. Although it is not a law that directly regulates speech, administrative detention can impact freedom of expression.

- **Right to Privacy**

a. The Counterterrorism Act of 2016. This law includes broad counter-terrorism measures, including provisions related to online content. The law gives the Israeli authorities the power to issue orders to remove content deemed to support terrorism, which may require surveillance and interference with individuals' digital activity. It also requires digital platforms to cooperate to remove content, which may affect the privacy of individuals through the collection of data to detect suspicious activities.

b. The Counterterrorism Law of 2016. This law focuses on prohibiting any form of support or encouragement for terrorist organizations, including in the online space, and penalizes any content creator that supports or promotes terrorist organizations, which may require monitoring and inspection of digital content, which may affect the personal privacy of individuals who post or share suspicious content.

c. Cybersecurity Act of 2015. This law relates to the protection of the national infrastructure against cyber threats. It covers issues related to the management of digital content. The law requires companies and other organizations to protect their systems against cyber threats and report any security incidents, which may include gathering data on users' digital activities. This law gives the prime minister the power to appoint employees to the **Israeli National Cyber Directorate** in secret and without a formal recruitment process, giving employees immunity from prosecution or even complaint, which could interfere with the privacy of individuals if strict safeguards are not in place.

d. Encryption and Privacy Act of 2005. This law regulates the use of encryption to protect personal information; although the law aims to protect data from unauthorized access, the application of encryption requires the collection and storage of information, which may interfere with privacy if not applied in a balanced manner.

e. The Computer Act of 1995. The law prohibits snooping and invasion of privacy using a computer. Article 4 states: "A person who unlawfully penetrates computer material located in a computer, shall be liable to imprisonment for a period of three years; for this purpose, 'penetration into computer material' – penetration by means of communication or connection with a computer, or by operating it, but excluding penetration into computer material which constitutes eavesdropping under the Eavesdropping Law, 5729-1979."

- **Right to Access Information**

a. Freedom of Information Act of 1998. This law aims to promote transparency in the work of public institutions and grants the public the right to access information held by government agencies. Article 1 states: "Every Israeli citizen and resident has the right to obtain information from a public authority."

b. The Protection of Privacy Law of 1981. This law regulates how personal data is processed and protected, including how to access this information in accordance with the rights of individuals. Article 1 of the law states: "No person shall infringe the privacy of another without his consent." Article 8 states:

a) No person shall manage or possess a database that requires registration pursuant to this section, unless one of the following has occurred:

(1)The database is registered in the Register;
(2)An application has been made to register the database and the provisions of sections 10(B1) have been met;
(3)The database requires registration pursuant to subsection (e) of the Registrar's order permitted management and possession of the database until the time of its registration.
(b) A person shall not use information in a database that requires registration under this section except for the purpose for which the database was established.

c. Public Records Act of 1958. This Act regulates access to public records and documents held by government agencies and specifies how to request and retrieve such records.

d. Criminal Procedure Act of 1982. This law includes rules on access to information related to criminal proceedings and investigations and guarantees the rights of individuals during these proceedings. Articles 73 through 79 make it clear that each defendant and his lawyer must be allowed access to all evidence that has been used as investigative material to bring charges. Article 78 clarifies that the accused and his or her lawyer can be denied access to "confidential material" but cannot rely on this evidence to bring charges.

The Criminal Procedure (Arrest and Search) Order of 1969: Article 23 of the law clarifies that searches in private homes and yards for the purposes of investigating a crime shall be ordered by the competent court. Article 23a clarifies that searching computers and other smart devices is also considered a search and must be carried out by computer specialists and only on the basis of a court order that clearly spells out what is to be searched (i.e., not everything can be searched) so as not to violate privacy. The 1979 Wiretap Act does not apply to this type of search.

Article 25a clarifies some of the exceptions that allow the police to search without a court order, such as believing that a crime is taking place at as premises, requesting assistance from someone inside the premises, or in the case of pursuing a fugitive. Paragraph b of this article, which applies from 15.05.2023 to 30.06.2025, states:

A police officer may, without a search warrant, enter and search any house or place if
(1) a reasonable suspicion arises that there is a weapon or substantial part of a weapon in the house or place that could be used as evidence of an offense under Section 144 (possession of a weapon without a license) of the Penal Code, if no action is taken. Failure to search immediately would frustrate the purpose of the search, and a search warrant cannot be obtained as the search must be conducted immediately to prevent the disappearance or damage to evidence.

Eavesdropping Prevention Act of 1977: Section 1: Unlawful eavesdropping and unlawful use of wiretapping. Article 2 states:

a)An eavesdropper without legal authorization shall be sentenced to five years' imprisonment.
b)A person who knowingly uses information or a conversation program obtained by eavesdropping, without legal authorization, whether lawfully or unlawfully, or knowingly discloses the information or content of that conversation to an unauthorized person, shall be sentenced to five years' imprisonment.

Article 4 states:

(a) The Minister may, if requested in writing by the head of the security authority, and if, after considering the extent of the invasion of privacy, he is satisfied that it is necessary for reasons of national security, authorize in writing the interception of telephone conversations.
(2) Reasonable suspicion has arisen that there is documentation or a camera in the home or place that may be evidence of the commission of a serious crime or offense under sections 144a, b or 340a(b) of the Penal Code, if failure to conduct a search immediately would frustrate the purpose of the search, and it is not possible to obtain a search warrant because it is necessary to conduct the search immediately to prevent loss of or damage to the evidentiary objects.

a. The National Security Protection Act of 1986. This law regulates how government agencies handle sensitive information that may affect national security and sets limits on access to such information.

b. The Security Information Act of 2007. This law addresses security information and how it is handled, including rights and restrictions on access to sensitive security information.

For a full list of limitations to the Right of Freedom of Expression in Israeli laws, please see Annex 1.

2.Palestinian National Authority

- **International Human Rights Law**

Under international human rights law, the State of Palestine is bound by a number of international treaties that aim to promote and protect human rights within its territory. These obligations are an essential part of its responsibilities as a state within the international community, whereby it pledges to comply with internationally recognized human rights, standards, and principles. These obligations focus, in particular, on treaties to which Palestine has acceded that play an important role in protecting international human rights.

One of these treaties is the International Covenant on Civil and Political Rights (ICCPR), which the State of Palestine acceded to on April 2nd, 2014. The ICCPR addresses a range of rights that have bearing on digital rights, including the right to freedom of expression, the right to access information, and the right to privacy. ICCPR is one of the foundational human rights treaties and sets out the obligations of state parties to ensure respect for, and the protection of, civil and political rights. The ICCPR institutes a legal framework that requires Palestine, as a signatory, to take all necessary measures to ensure compliance with its standards.

The International Covenant on Economic, Social and Cultural Rights (ICESCR) is another treaty that is considered an essential part of the international human rights framework. It, too, was signed by the State of Palestine on April 2nd, 2014. This treaty sets out a framework of obligations addressing the economic, social, and cultural rights of individuals, as well as the right to education as one of the digital rights that will be addressed in this research. The Covenant obligates states parties to work to improve economic, social and cultural conditions in accordance with available resources.

In this context, it is important to highlight the concept of ‘effective control’ as key to a state’s capacity to fulfill obligations under international human rights law. Effective control is a key concept in international law that refers to the ability of a state to exercise authority and administration over its territory and population effectively. In the context of the State of Palestine, effective control imposes a certain framework for its obligations under international treaties. According to international legal principles, a state is obligated to implement human rights only within the scope of its effective control. In the case of the State of Palestine, this means that the State has the responsibility to implement human rights in territories and areas where it has effective control, while it may face challenges fulfilling this obligation in areas it does not fully control or where political and economic circumstances constrain it. This limited applicability of obligations does not absolve Palestine of its responsibilities but limits the extent of its obligations according to its actual capacity to fulfill them.[27]

[27] Office of the United Nations High Commissioner for Human Rights, 2022

- **Palestinian Law Relating to Digital Rights**

Palestinian law does not explicitly regulate digital rights. However, many laws regulate the broader rights examined in this study.

The Palestinian Basic Law enshrines the basic rights of freedom of expression and privacy. Article 10 affirms that human rights and fundamental freedoms are binding and must be respected, and mandates that the Palestinian National Authority accede to charters that protect human rights. Article 11 states that personal freedom is a guaranteed natural right and may not be restricted except by judicial order in accordance with the provisions of the law. Article 19 guarantees freedom of opinion and expression, stating that any individual has the right to express and disseminate their opinion by any means, subject to the provisions of the law. Article 27 emphasizes the right to establish newspapers and other media outlets and prohibits censorship except by court order. Article 32 provides protection against attacks on personal freedoms and privacy and guarantees fair compensation for those affected. Articles 110 and 111 specify the conditions and limitations of rights during a state of emergency, indicating that rights and freedoms may be restricted only to the extent necessary to achieve a specific, necessary goal.

Numerous laws enshrine rights in the digital space, such as privacy, freedom of opinion and expression, and access to information, either explicitly or implicitly. These are discussed next.

- **Right to Freedom of Expression**

a. Palestinian Basic Law

The Palestinian Basic Law protects the right of individuals to express their opinion. Article 19 states: “Freedom of opinion shall not be violated. Every person has the right to express and disseminate his opinion orally, in writing, or through other means of expression or art, subject to the provisions of the law.” Article 27 of the Basic Law grants the right to establish newspapers and other media outlets and guarantees the freedom to produce audio-visual and written media, to print, publish, distribute and broadcast, and the freedom of those employed by the media.

b. Cybercrime Law No. 10 of 2018

The Cybercrime Law addresses the right to freedom of expression. Article 21 states:

1. Every human being shall have the right to express his opinion by speech, writing, photography, or other means of expression and publication in accordance with the law. 2. The freedom to artistic and literary creativity shall be safeguarded. Legal proceedings may not be instituted or brought for the halt or confiscation of works of art, literature or intellect or against their innovators except by a court order. A penalty of deprivation of liberty or a custodial sentence may not be imposed in crimes, where are committed because of the publicity of the artistic, literary or intellectual production. 3. Freedom of the press, printing and paper-based, audio-visual and electronic media is safeguarded. Palestinians, including natural and legal persons, public and private, have the right to own and issue newspapers, and establish audio-visual media outlets and digital media in accordance with the law. 4. Restrictions may not be placed on the press, nor may it be seized, halted, warned or eliminated, except in accordance with the law and under a court decision.

The Cybercrime Law also includes several provisions that could be exploited to restrict freedom of expression. For example, Article (39) states:

1. The competent authorities of investigation and seizure, in the event they monitor hosted electronic websites, which broadcast either inside or outside the State, posting any expressions, figures, images, films, propaganda materials or others which may threaten national security, public order or public morals, shall be entitled to submit a report thereon to the Attorney General or one of his assistants and request permission to block the broadcast of the electronic website(s) or block some of their links. 2. The Attorney General or one of his assistants shall submit the application for permission to the Court of Conciliation within 24 hours, enclosed with a notice of his opinion. The Court shall render its decision on the application on the same day it is brought before it, stating either acceptance or rejection, provided that the duration of the blockage does not exceed six months unless the duration is extended in accordance with the procedures provided for under this Article.

c. Printing and Publishing Law No. 9 of 1995

Article 2 of the Printing and Publishing Law reaffirms the provisions of the Basic Law for freedom of the press, printing and freedom of expression. Article 4 of the law defines the scope of freedom of the press as follows:

Informing citizens of facts, ideas, trends, and information at the local, Arab, Islamic, and international levels. d. Allowing citizens to publish their opinions. C- Searching for information, news and statistics of interest to citizens from its various sources, analyzing, circulating, publishing and commenting on them within the limits of the law. D. The right of the press publication, news agency, editor and journalist to keep the sources of information or news obtained confidential unless the court decides otherwise during the consideration of criminal cases in order to protect state security, prevent crime or achieve justice.

Article 7 of the law stipulates the limits of the freedom of publication, which consists of refraining from publishing what is “contrary to public order” and specifies the controls for this in paragraph (a), which states:

Publications must refrain from publishing anything that contradicts the principles of freedom, national responsibility, human rights and respect for the truth, and consider freedom of thought, opinion, expression and information as a right for citizens as well as for themselves.”

Paragraph (b) states:

Periodicals aimed at children and adolescents must not include any pictures, stories or news that violate Palestinian morals, values and traditions.

- **Right to Privacy**

a. Cybercrime Law No. 10 of 2018

The Cybercrime Law guarantees the right to privacy under Article 22, which prohibits unlawful interference in the privacy of individuals, including their family affairs and correspondence. The article imposes a penalty of imprisonment of not less than one year or a fine of not less than JD 1,000 on anyone who creates a website, application, or electronic account or publishes information on the Internet or any other form of information technology with the intention of publishing news, images, or audio or video recordings – whether live or recorded – that constitutes unlawful interference in the private or family life of individuals. Article 32 regulates the powers of the Public Prosecutor regarding the search of persons, places, and information technologies when investigating a specific crime: the Article stipulates that the search order must be reasonable and specific and makes provision for the renewal of the order if justified.

The Article grants the Public Prosecutor the authority to authorize the direct access of judicial officers or officially appointed experts to any information technology system and to conduct a search to obtain data or information; the judicial officer must be qualified to deal with the special nature of cybercrime.

b. Penal Code No. 16 of 1960

The Penal Code safeguards the right to privacy by imposing sanctions on behaviors that infringe such privacy. Article 365 regulates the duties of employees of the cable and postal services. It states:

“all persons working with the cable, post, and telecommunication services, who have access to sensitive and private information, shall comply to safeguarding the privacy of such information that come to their knowledge through their work. Any person who works for the cable or postal services and misuse the duties of his/her job by viewing sealed letters or destroying or embezzles a letter or reveals its content to another person other than the addressee, he/she shall be punished by imprisonment from one month to one year. Moreover, any person who works for the telecommunications services and by reason of his / her office reveals the content of a phone call; he / she shall be punished by imprisonment for six months or a fine up to twenty dinars (JD20).”

c. Law of Penal Procedures No. 3 of 2001

Article 51 of the Law of Penal Procedures protects the right to privacy of suspects in criminal cases. The law grants special powers to the office of the Public Prosecutor to view and seize letters, communications, newspapers, printed matter, parcels, and telegrams at postal and telegraph offices if relevant to a case. It also grants the Public Prosecutor the power to tap telephone and wireless communications, and record conversations conducted in a private place. if authorized by a conciliation judge on the ground that it may yield evidence in a felony or a misdemeanor punishable by imprisonment for a term of not less than one year. Paragraph 3 of Article 51 strengthens the protection of privacy by stipulating that there must be reasonable grounds for authorization for seizure, surveillance, or recording and the authorization must be limited to a period not exceeding fifteen days, with provision for one extension of this period.

It should be noted that the Law of Penal Procedures applies “proportionality and necessity criteria” to protect the digital right to privacy of suspects in a criminal investigation.

d. Council of Ministers Decision No. 3 of 2019 on the Personal Data of Citizens

While this decision does not address the right to privacy explicitly, it prohibits the direct or indirect use of personal data obtained from companies and service providers for commercial purposes without individuals’ consent, under penalty of legal liability.

- **Right to Access Information**

The right of access to information is closely linked to the right to freedom of expression: if freedom of expression is censored, preventing the publishing of information or opinions, the right of individuals to access that information is subsequently curtailed.

Palestinian law does not address the right to access information explicitly, but this right is implied with limitations in several laws.

- **Palestinian Basic Law**

Article 29 of the Palestinian Basic Law guarantees the freedom of the press and the media and recognizes the right of any individual to establish a newspaper or media house and to print, publish, distribute and transmit. It prohibits the imposition of any form censorship on the media, including warnings, suspension, confiscation, cancellation, or other restrictions, except in accordance with legal provisions and judicial authorization, thereby promoting the right to access to information. In addition, Article 6 of the Basic Law stipulates that official bodies must facilitate the task of journalists and researchers in accessing their programs and projects, which increases the effectiveness of oversight and accountability. Despite these guarantees, the Basic Law lacks explicit provisions guaranteeing freedom of access to information. This constitutes a loophole that may be used to limit access to information.

- **Publications and Publishing Law No. 9 of 1995**

Article 2 of this law guarantees the freedom of the press, the freedom to print, and freedom of expression, whether through speech, text, or visual media. Article 4 enshrines the right of citizens to access information and ideas from a variety of sources, and to research, analyze, and publish news and statistics, while maintaining the confidentiality of information sources, except by order of the court. Article 6 obligates official bodies to facilitate access of journalists and researchers to their programs and projects. However, the law imposes several restrictions on these rights: Articles 7 and 37 stipulate the conditions for publishing information, which may restrict the freedom of the press and media and limit their effectiveness, negatively impacting citizens' access to information.

- **Civil Affairs Law No. 2 of 1999**

Article 7 of the Civil Affairs Law guarantees the right of citizens to obtain documents related to themselves or to their family line, at a fee. Article 10 prohibits the publication or disclosure of these documents to unauthorized parties, except by order of the court, and prohibits the removal of records from official archives.

- **Law of Penal Procedure No. 3 of 2001**

Article 59 of the Law stipulates that any information obtained during an investigation, and the methods used to obtain it, must be kept confidential; sharing this information is a crime punishable by law. Article 237 provides that the trial shall be public unless the court decides to conduct it in camera for reasons of public order or morality, to promote transparency and to ensure justice. Trials may thus be held in camera in specific exceptional cases.

- **Anticorruption Law No. 1 of 2005 (as amended)**

Article 8 of this Law mandates the Anti-Corruption Commission (ACC) to monitor the financial activity of government officials to enhance transparency and accountability. The powers of the ACC include collecting and monitoring all financial disclosures by officials and investigating corruption cases. Article 9 grants the ACC the authority to gather information from records and documents, summon witnesses, and coordinate with government bodies. The law requires the ACC to publish an annual report on its activities to promote the right of the public to transparency. Some investigations carried out by the ACC may be kept confidential, however, to protect whistleblowers and facilitate access to relevant information. Thus, the law strikes a balance between ensuring transparency in the ACC’s work and protecting the individuals involved in investigations.

- **General Statistics Law No. 5 of 2000:**

The General Statistics Law enhances citizens' right to access information at many levels. Article 4 stipulates that all individuals have a right to access the official statistics collected, processed, and disseminated by the General Bureau of Statistics, in accordance with the adopted roles and instructions, with due consideration for the confidentiality of data and individuals' privacy.

The right of citizens to access information is promoted through several key aspects. First: Article 4 states that all members of society have the right to access official statistics collected by the Palestinian Central Bureau of Statistics, taking into account the confidentiality of data and the privacy of individuals, which guarantees citizens access to information that reflects social, economic, and environmental realities. Secondly: Article (3) of the law requires the PCBS to provide accurate official statistics on conditions and trends in various fields, including the issuance of an annual statistical book that allows citizens to access and analyze the collected data. Third: The agency cooperates with educational and research institutions to provide the necessary information and statistics, which contributes to spreading knowledge and providing data to researchers, decision makers, and citizens. Finally, Article 17 of the same law stipulates that all individual information remains confidential, and statistics must be published in the form of aggregate tables only, which strikes a balance between transparency and privacy protection, and allows citizens to access the necessary information without compromising their privacy. Through these articles, the law promotes transparency and guarantees citizens access to important data and information while maintaining the protection of privacy and confidentiality of personal data.

For a full list of limitations to the Right of Freedom of Expression in Palestinian laws, please see Annex 2.

5. Practices of Israel as the Occupying State

A widespread pattern of censorship, surveillance, legal persecution, and physical targeting, particularly in relation to online expression, access to information, and journalistic activity were practiced against Palestinians. Multiple organizations and monitoring bodies—including Human Rights Watch, Adalah, 7amleh, Al-Haq, and others—have reported on these violations across social media platforms and digital communication networks. The violations cover a range of rights, including freedom of opinion and expression, the right to privacy, gender-based protections, access to the internet, and the safety of journalists, indicating a broader suppression of Palestinian digital presence and civic space. The following table presents documented digital and media rights violations affecting Palestinians from October 7th, 2023, to October 7th, 2024.

	Right Violated	Evidence
1	**Right to freedom of opinion**	From October 7th, 2023, to July 1st, 2024, over 1,350 cases of censorship of content related to Palestine on social media platforms and networks were documented. These included suspension of accounts, removal of content, and limiting reach. Instagram and Facebook were responsible for the largest number of cases, followed by TikTok, X, and YouTube. Among those affected were more than 150 media outlets. During the same period, the Palestinian Observatory for Digital Rights Violations (Hurr) documented a total of 3,325 violations in the form of violent content across various social media platforms. The largest number of cases occurred on Facebook, with 1,366 cases, and X, with 1,297 cases, with cases also documented on Instagram, Telegram, and other platforms. Seventy-three percent of the cases were categorized as instances of incitement; the rest were categorized as hate speech, defamation campaigns, and other forms of harmful content.[28]
2		During October and November 2023, Human Rights Watch documented more than 1,050 instances of content supporting Palestinian rights or reporting human rights violations removed or otherwise restricted on Instagram and Facebook; only one of these posts contained violent content.[29]
3		While a survey conducted in 2019 by the Hamama Center found that over a third of respondents (1,200) had been subjected to legal accountability as a result of expressing their opinions in the network, a survey conducted by the Centre in 2024 showed that more than half of the respondents (449) had been subjected to legal accountability by the Israeli authorities, and nearly 60% had been subjected to similar accountability by the Palestinian Authority. The 2024 survey found that almost equal percentages faced pressure to delete political and social posts from Palestinian security services (80.2%) and Israeli security services (82.9%).[30]
4		Adalah reported that between October 7th, 2023, and March 27th, 2024, Israeli police arrested 401 people on charges related to freedom of expression.[31] A press release issued by the Israeli Police on May 1st, 2024, stated that 162 indictments had been issued for “incitement to terrorism.” In its monitoring, Adalah found that a large majority of these indictments targeted Palestinian citizens of Israel and residents of East Jerusalem. The number of indictments show a marked upward trend: for the five-year period 2018 through 2022 only 84 indictments were filed.[32]

[28]- 7amleh, The Arab Center for Social Media Development, Report on Palestinian Digital Rights, Genocide, and the Responsibility of Major Technology Companies, September 2024."
https://7amleh.org/storage/genocide/Arabic%20new.pdf

[29] Human Rights Watch. Meta’s Broken Promises, Systemic Censorship of Palestine Content on Instagram and Facebook-.20 December 2023. https://www.hrw.org/news/2023/12/20/meta-systemic-censorship-palestine-content

[30] Campaign, Arab Center for Community Media. The War on Gaza: An Analytical Reading on the Consequences and Effects on the Digital Security of Palestinian Youth. 3 September 2024.

[31] Adalah’s report to the UN Special Rapporteur on Freedom of Opinion and Expression Threats to Palestinians’ FoE rights in Israel post-7 October 2023. 30 June 2024.

[32] Institute for Palestine Studies. "Adalah: One Year After the War on Gaza: Deepening Apartheid and Undermining the Citizenship of Palestinians in the Interior." Published on October 10, 2024. See the following link: https://shorturl.at/lQw7B

5		After October 7th, 2023, during Israel's assault on Gaza, 35 Israeli universities and colleges initiated disciplinary proceedings against some 160 Palestinian students for posts on their personal social media accounts.[33]
6		Since October 7th, 2024, Al-Haq has documented 10 violations, distributed among 6 violations by the occupation, which included Israeli soldiers beating and attacking Palestinians at checkpoints as a result of sharing some publications, banning news channels, attacking journalists and restricting their work, as well as firing an employee on the grounds of sharing a publication, During the same period, Al Haq documented 4 violations by the Palestinian Authority related to freedom of opinion and expression or sharing publications and other related violations. [34]
7		From October 7th to November 14th, 2023, Israel's Cyber Unit issued 9,500 takedown requests to social media platforms, with 60% directed to Meta; there was a 94% compliance rate[35].
8	**Right to privacy**	**Sada Social** monitored privacy violations on Messenger, where messages related to Palestinian affairs were blocked or automatically deleted. Although WhatsApp identifies itself as an encrypted app, more than 700 Palestinian numbers were blocked; of these, more than 76% were from the Gaza Strip, adding to the challenges individuals in Gaza faced amid the communications blackout.[36]
9	**Digital gender-based violence**	A survey conducted by 7amleh Center found that 50% of female participants felt that they are being monitored by social media; 28% of female respondents reported having been victims of an attempt to hack their accounts on social media and 25% mentioned they endured harassment, ridicule, or scrutiny comments for being women.[37]
10	**Access to the Internet and targeting of networks**	NetBlocks reported that since the beginning of the Israeli military campaign on Gaza Palestinians have experienced at least 15 telecommunications outages. In 2023: October 27th to 29th; October 31st to November 1st; November 5th to 6th; November 16th to 17th; November 4th to 5th; December 14th to 17th; December 20th to 21st; and December 26th to 27th. In 2024: January 12th to 19th; January 22nd to 24th; March 5th; March 12th; April 12th; May 12th; and May 25th [38]

[33] Adalah's Report to the UN Special Rapporteur on the Right to Education Israeli Academic Institutions Sanction Palestinian Students for Social Media Posts since 7 October, violating their Rights to Free Expression and Education. 15 February 2024.

[34] Al-Haq Institute, email correspondence on 22 September 2024.

[35] Digital Apartheid in Gaza: Unjust Content Moderation at the Request of Israel's Cyber Unit. July 26, 2024. https://www.eff.org/deeplinks/2024/07/digital-apartheid-gaza-unjust-content-moderation-request-israels-cyber-unit

[36] SadaSocial. A Year of Digital Genocide on Palestinians to Digitally Reproduce the Tools of Genocide on Palestinians October 7, 2023. 6 October 2024.

[37] 7amleh, Arab Center for Social Media Development. Guide to Combating Gender-Based Digital Violence. 24 December 2023.

[38]- The source: NetBlocks and Radar Cloudflare, live updates on X platform, last accessed on July 14, 2024, available at: www.x.com

11		As of October 31st, 2024, 15 out of 19 service providers in Gaza had faced a complete shutdown of mobile phone and high-speed internet services, while the remaining four faced varying, but significant, levels of disruption, affecting millions of people. Some 411,000 people using the services of these providers in Gaza were directly affected by the complete shutdown, in addition to another 34,000 people in the West Bank.[39]
12		From October 2023 to October 7th, 2024, the Gaza Strip has experienced repeated and deliberate interruptions of telecommunications and internet services by the Israeli occupation, with over 10 instances of complete loss of service and other instances of interruption of service to some areas, including Jenin, pushing it into digital darkness as a result of targeting the main and backup telecommunications lines.[40]
13		Since the beginning of Israel's 2023 assault on Gaza, the Israeli military has deliberately and systematically targeted Gaza's telecommunications infrastructure. The Palestinian Central Bureau of Statistics (PCBS) reported that this resulted in at least 10 complete disruptions of telecommunications services by mid-April 2024, and 75% of Gaza's 841 telecommunications towers out of service[41].
14	**Violations against journalists**	From October 7th, 2023, to October 7th , 2024, 174 journalists were killed and 108 arrested in the West Bank, Gaza Strip and Jerusalem, some as a result of their activity on social media platforms.[42]

Restrictions to Access to Internet:

As established previously in this document, Israel, as an occupying state, is legally obligated to provide Internet to the Palestinian territories under occupation in accordance with international human rights law, international humanitarian law, and the Oslo Agreement between Israel and the Palestinian National Authority.

Since its occupation of Palestinian territories in 1967, Israel has controlled the ICT sector in these territories – first, directly through its Ministry of Communications, and later under the management of Bezeq, Israel's national telecommunications company. In 1995, under the Oslo Accords, Israel transferred partial control of the ICT infrastructure in the West Bank – excluding East Jerusalem – and the Gaza Strip to the Palestinian Authority. The agreements divided the political geography of the West Bank into three areas: Area A, which constitutes 18% of the West Bank, was placed under control by the Palestinian Authority; Area B, which constitutes 22% of the West Bank, was placed under Palestinian civil control with joint Palestinian Israeli security control; and Area C, which constitutes 60% of the West Bank, was retained under full Israeli control. In East Jerusalem, the ICT infrastructure remains under full Israeli control and no Palestinian operator is permitted to provide services there.

[39] 7amleh, The Arab Center for Social Media Development, Report on Palestinian Digital Rights, Genocide, and the Responsibility of Major Technology Companies, September 2024."
https://7amleh.org/storage/genocide/Arabic%20new.pdf
[40] https://sada.social/ar/post/aaam-mn-albad-alrkmy-llflstynyyn
[41] Joint press release by the Palestinian Bureau of Statistics and the Ministry of Communications and Digital Economy on the Occasion of World Telecommunication and Information Society Day, which falls on May 17th https://www.pcbs.gov.ps/postar.aspx?lang=ar&ItemID=5756
[42] https://sada.social/ar/post/aaam-mn-albad-alrkmy-llflstynyyn

Although Israel has illegally annexed East Jerusalem and implemented its civil law there, under international law East Jerusalem remains occupied territory.[43]

The first Palestinian mobile operator in the West Bank and Gaza Strip was Jawwal. It obtained a license to operate in 1998 and began providing services on frequencies including 2.4 megahertz (MHz) exclusively and 2.4 MHz shared in the 900 MHz band, with approximately three million subscribers[44]. In 2000, the Palestinian Ministry of Telecommunications and Information Technology requested that Israel release frequencies for the entry of the second Palestinian operator, Wataniya, into the market. Israel, however, failed to respond to this request. In 2007, the Ministry granted a license to Wataniya, despite the lack of access to frequencies, and provided it with licenses for second-generation (2G) and third-generation (3G) mobile phones.[45] Israel released a limited number of frequencies, including 3.6 MHz in the 900 MHz band and 2.8 MHz in the 1800 MHz band, which were not allocated exclusively to Wataniya, but were also available to Israeli operators. Subsequently, Wataniya began operating in the West Bank in November 2009, and in the Gaza Strip in 2017, after a second release.[46]

Israel has continued to reject requests by the Palestinian Authority for permission to deploy new technologies in the field of information and communications technology. More than a decade after the first request to launch 3G frequencies was submitted, the service became available in the West Bank in early 2018. Israel also prevented the deployment of WiMax (Universal Compatibility Microwave Access) systems, which provide access to high-speed wireless networks for rapid data transfer, which was intended to enable communication anywhere, anytime and from any device.[47]

Mada[48] reports that the provision of internet service in Palestine encounters challenges at all stages – from importing equipment to operating and maintaining the network – due to restrictions imposed by the Israeli occupation that negatively affect efficiency and costs. The most serious of these challenges are as follows:

a. Importing equipment needed to build the internet network: The occupying power imposes strict restrictions on Palestinian internet service providers regarding the selection of equipment suppliers, as it is prohibited to import equipment from certain companies – such as the Chinese company Huawei, despite its high quality and lower cost. This forces Palestinian companies to import equipment at higher costs and of lower quality, which increases the cost of building networks.

b. Obtaining frequency licenses for mobile internet services: The process of obtaining frequency licenses for 2G, 3G, and 4G is unjustifiably long and expensive. In most countries, unified licenses are granted for multiple-generation services, while Palestinian companies must obtain separate licenses for each generation, which hinders the efficient provision of the service.

c. Use of frequencies and access to the Internet: Palestinian companies are required to provide extensive documentation to the occupation authorities, creating heavily bureaucratic hurdles in order to operationalize networks.

[43]- Musleh, David. “Information and Communication Technology in Palestine: Challenging Constraints and Power Dynamics”. Published by Al-Shabaka (Arabic), January 2022. Check the following link: https://shorturl.at/oJVGe

[44] General Union of Palestinian Economist. “Palestinian Communications and Frequency Spectrum”. Published on May 16, 2017. Check the following link: https://shorturl.at/uq2Ln

[45]- Ibid

[46]- Ibid

[47]- Personal interview with a respondent from one of the private sector companies who declined to have their name listed as a reference.

[48] Personal interview with Adel Al-Aloul, representing Mada. 4 September 2024.

d. Providing internet access via a fiber connection: Palestinian companies rely on the Israeli company Bezeq for internet service, as the Internet is transmitted from Haifa to Ramallah and Gaza. This process imposes double costs on companies, including the cost of purchase and transportation.

e. Israeli surveillance of Palestinian networks: Palestinian networks face indirect surveillance by the occupation authorities, which affects the freedom of network operation and data confidentiality.

f. Challenges of connecting the fiber network in the West Bank: Palestinian companies have attempted to establish a comprehensive fiber network in the West Bank, but the Israeli occupation authorities have obstructed the installation of a fiber line extending 5 meters above Road No. 5, which passes near illegal Israeli settlements, that is necessary to complete this connection.

g. Difficulty providing internet access in areas classified as 'C': Palestinian companies face major challenges obtaining the necessary security approvals to provide internet service to areas that fall under Area C and are under complete Israeli control.

In August 2023, Mada was given permission by Israel to bring fiber optic internet cable into the West Bank, with heavy documentation requirements. Fiber internet service is not yet operational in Gaza, however.

- **Changes to internet access since October 7th,2024:**

.

o Gaza Strip:

- Damage to internet infrastructure as a result of Israel's military assault has interrupted service provision. [49]
- Despite damage to infrastructure, Mada continued to provide internet service free of charge and cancelled outstanding accounts.

o West Bank:

- The internet infrastructure was destroyed in many areas, including in the Tulkarem, Nur Shams, and Jenin refugee camps,[50] causing significant financial losses.
- The Israeli occupation authorities deliberately delayed repairs to infrastructure and delivery of equipment, further impeding operational procedures.

These challenges highlight that the provision of internet services in Palestine requires extraordinary effort on the part of Palestinian companies due to the ongoing restrictions imposed by Israel. The telecommunications company Ooredoo also confirmed that the occupation imposes many challenges on them. Most impactful are: denial of the necessary frequencies to activate fourth-generation service; penetration of the Palestinian market by Israeli telecommunications companies; the inability to increase coverage and broadcasting in Area C as it falls under complete Israeli control and requires permits from Israel; and failure of Israel to grant approval in the necessary time to activate the fiber service to be dedicated to the company's use only. Ooredoo repeated increased difficulty obtaining approvals and the transfer of equipment since the beginning of Israel's assault on the Gaza Strip.[51]

Majdi Haj Khalil[52] , a telecommunications expert from the private sector, identified the following **major challenges facing the telecommunications sector** due to the restrictions imposed by Israel.

[49]- Jawwal telecom. "Telecommunications Group announces that the landline, mobile, and internet networks will be disrupted if the aggression continues". Check the link: https://shorturl.at/yhQyg

[50]- Live journalistic report via Al-Hadath TV channel. Check the link: https://linkcuts.com/dqf7npu2

[51] Email correspondence with Ooredoo Palestine, September 22nd, 2024

[52] Personal interview with Magdy El-Haj Khalil, private sector expert in the field of communications, September 23, 2024.

a. Infrastructure

Internet infrastructure in Palestine is constrained by many factors – most notably, the long bureaucratic processes involved with installation as a result of the Israeli occupation. Israel imposes strict restrictions on the entry of necessary equipment, such as cables and transformers, on the pretext that they are 'dual-use'– meaning that they may be used for communications or for military purposes, or because they may penetrate or affect Israel's military telecommunications networks.

Companies also experience difficulty connecting networks between Palestinian villages and cities due to the complexities of obtaining the necessary licenses. As a result, companies are forced to use longer routes for installation, which increases costs.

In the Gaza Strip, internet and telecommunications providers suffered huge losses as a result of the destruction of infrastructure during Israel's military assaults, which severely impacted the continuity of service and ability to restart networks.

b. Licenses

The Israeli occupation authorities complicate the process of obtaining the necessary licenses at every step in the process of providing internet and communications services. These hurdles relate to obtaining the necessary frequencies, approval to install internet towers and cable networks. Israel uses slow and bureaucratic processes with Palestinian applications. In many cases, there is no specific time frame for processing license applications, which may span several years.

c. Access to information via Palestinian networks

As Palestinian internet providers are forced to connected to the internet via an Israeli provider, the Israeli authorities have the means to access the data of Palestinian users, although the information is not directly filtered.

d. Uses of fiber internet connection in other sectors

In addition to its use in the telecommunications sector, fiber cables are employed in other industries, such as the banking sector, where fiber cables are used to connect ATMs and ensure that banking operations continue even in the event of a failure in the main Internet network.

Since the start of Israel's military offensive in Gaza on October 7th, 2023, telecommunications services and internet access have deteriorated significantly in the Gaza Strip. Evidence suggests that power outages across Gaza are the result of a combination of direct attacks on civilian communications infrastructure – including cell phone towers, fiber optic cables, and internet service provider offices – and restricted access to electricity resulting from attacks on infrastructure, denial of services, and blockades of the fuel needed to operate generators. Deliberate disruptions of telecommunications services by Israeli service providers have exacerbated the situation.[53]

Where connectivity is still available, it is unreliable in terms of quality and location. At the time of writing, residents of Gaza continue to lack access to a reliable and secure communications system with reliable connectivity.

[53] Access Now. #KeepItOn: Telecommunications blackout in the Gaza Strip is an attack on human rights, available at: https://bit.ly/3Y3fc2j , 13 October 2023.

According to an in-depth analysis by Access Now of the connectivity status of the main internet service providers in the Gaza Strip between the 4th and 31st of October 2023, 15 of the 19 service providers operating in Gaza experienced a complete shutdown of mobile and broadband services. The remaining 4 companies experienced significant but varying levels of outages, significantly impacting millions of people. As a result, internet traffic across Gaza dropped by more than 80% during October 2023. [54]

In addition to targeting and destroying internet infrastructure, Israel has targeted Palestinian telecommunications technicians and their crews as they carry out the repairs necessary to restore connectivity in Gaza. According to Paltel, its teams can only service the networks during ceasefires if they receive safe passage from the Israeli authorities, which is often not granted.[55]

Crews who have received approval to service infrastructure and have coordinated their movements with the Israeli military have also been attacked. On January 13th, 2024, an Israeli tank shelled a Paltel crew vehicle, killing two employees, Nader Abu Hajjaj and Baha al-Rayyes, as they returned from a mission to repair a damaged generator in Khan Younis[56]. A media investigation into the incident revealed that the attack was deliberate, and occurred despite Paltel coordinating with the Israeli military to provide safe passage, including receiving a detailed map from the Israeli military outlining the exact routes the crew was permitted to take[57] . It was reported that the Israeli military had previously targeted Abu Hajjaj while he was repairing cables and replacing batteries in a building in Khan Younis despite the coordination of his movements with the Israeli authorities[58].

In addition to the ongoing decline in connectivity across the Gaza Strip, Access Now documented at least fourteen complete internet and communications outages between October 2023 and May 2024. The duration of these outages varied from a few hours to more than a week. The first complete outage occurred started on 27th of October, 2023, and lasted for 36 hours amid unprecedented aerial bombardment as Israel prepared to launch its ground invasion of the Gaza Strip. The outage caused widespread panic and anxiety among the civilian population, emergency service providers, and the humanitarian organizations – including several UN agencies – operating in Gaza.[59]

Restrictions on the Right to Freedom of Expression

The right to freedom of expression, as a digital right, is enshrined in international human rights law and international humanitarian law; as demonstrated previously in this document, Israel, as an occupying state, is without question obligated to respect and protect this right, whether in digital space or physical space.

The Israeli occupation, however, systematically restricts the right of Palestinians to freedom of expression, entrenching this through domestic legislation which, in contravention of international law, it applies to the territories it occupies. The illegal application of Israeli law in East Jerusalem and military orders in the West Bank directly contribute to the legitimizingby Israel of the violation of Palestinians' right to freedom of expression, which constitutes a violation of human rights – especially Article 19 of the International Covenant on Civil and Political Rights and other rights related to this right – such as the right to peaceful assembly, the right to access information, and the right to access justice.

[54] Access Now, Palestine unplugged: How Israel disrupts Gaza's internet, available at: Palestine unplugged: how Israel disrupts Gaza's internet - Access Now 10 November 2023.
[55] The New York Times, These WorkersAre Risking Their Lives to Restore Gaza's Phone Network, available at: https://nyti.ms/4eDKxjt , 13 March 2024.
[56] See Jawwal's statement on 13 January 2024: https://twitter.com/JawwalPal/status/1746218633221591108
[57] +972 Magazine. A Gaza team went to repaira telecoms machine.An Israeli tank fired at them, available at: https://bit.ly/4h2Vxlu , 1 May 2024
[58] Ibid.
[59] The New York Times, 34 Hours of Fear: The Blackout That Cut Gaza Off From the World, available at: https://bit.ly/4eMBuwl 29 October 2023.

On September 16th, 2024, several Palestinian civil society organizations concerned with human rights met to discuss developments in the Palestinian digital rights landscape from October 7th, 2023, to September 1st, 2024. The meeting was attended by ***the Arab Center for the Development of Community Media (7amleh), Human Rights Watch, Al-Haq Institute, the Independent Commission for Human Rights, the Jerusalem Legal Aid Center, and MIFTAH.*** The group evaluated **Israel's measures and practices to restrict the freedom of expression of Palestinians** as follows:

1. Arrest and administrative detention:

These measures were used to restrict freedom of expression on the basis of Israeli domestic law illegally in force in East Jerusalem and military orders in force in the West Bank. Since the outbreak of the war on October 7th, 2023, the Israeli police have launched a large-scale arrest campaign against the Palestinian residents of East Jerusalem. These arrests were based on accusations of "incitement to terrorism" and "membership in a terrorist organization," based on individuals' posts on social media. These charges invoked Article 24 of the Israeli Anti-Terrorism Law of 2016, which stipulates a prison sentence of up to three or five years, depending on the nature of the crime. Since this law was enacted, many human rights organizations have expressed concerns about its terms, which have been described as vague and overly broad, opening the way for its arbitrary and selective implementation for illegitimate political purposes, thus enabling further suppression of Palestinians' right to freedom of expression.

2. Incitement and persecution:

A widespread campaign of incitement and persecution by Jewish Israelis – including the Prime Minister, several officials, and other influential figures – has been carried out both online and offline against Palestinians without legal consequences[60].

These campaigns have resulted in the imprisonment of large numbers of Palestinians, with 389 of the 401 detainees held for more than 24 hours. According to a statement from an official in the State Attorney's Office, the state's "zero tolerance approach" has led to approximately 80% of these cases ending with individuals being held without bail until the end of legal proceedings, which can last for months and can be extended by a decision of the Supreme Court. In addition, the Israeli police have subjected hundreds of Palestinian traffic officers to interrogation and warnings based on their activity on social media and other forms of expression. The police have also recorded numerous cases of illegal arrests, on charges such as "behavior that is likely to disturb the public peace" according to the Israeli Penal Code, particularly in the context of demonstrations and activity on social media.[61]

In February 2023, Israeli National Security Minister Ben-Gvir, who has direct authority over both the Israeli police and prison system, established a dedicated unit within the police force to "combat incitement to terrorism on social media[62]." The unit monitors social media, refers cases it deems illegal for arrest, and reports posts on social media platforms for removal, undermining Palestinians' freedom of expression.

[60] Adalah's report to the UN Special Rapporteur (SR) on Freedom of Opinion and Expression: Threats to Palestinians' FoE rights in Israel post-7 October 2023. Submitted 30 June 2024.

[61] Adalah's report to the UN Special Rapporteur (SR) on Freedom of Opinion and Expression :Threats to Palestinians' FoE rights in Israel post-7 October 2023. Submitted 30 June 2024,

[62] Haaretz, Netanyahu Taps Ben-Gvir to Head Team 'Fighting Terror Incitement by Palestinians' 19.Feb,2023 Netanyahu Taps Ben-Gvir to Head Team 'Fighting Terror Incitement by Palestinians' - Israel News - Haaretz.com

3. Use of disciplinary proceedings:

Since the start of Israel's current assault on Gaza launched on October 7th, 2023, 34 Israeli universities and colleges have initiated disciplinary proceedings against approximately 160 Palestinian students holding Israeli passports, who are studying at Israeli universities and colleges, due to posts on their personal social media accounts. The academic institutions initiated these proceedings following complaints filed by far-right Jewish Israeli student groups and other students. The disciplinary proceedings taken by Israeli academic institutions after October 7th are unprecedented in scope and subject matter, significantly impacting the rights of Palestinian students, including freedom of expression. These policies have targeted Palestinian students almost exclusively and have been explicitly endorsed by Israeli Education Minister Yoav Kisch.[63]

In March 2024, renowned Palestinian feminist and scholar at Hebrew University, Professor Nadera Shalhoub-Kevorkian, was suspended from teaching after signing a petition accusing Israel of committing genocide in Gaza and following accusations by Hebrew University regarding remarks she made on a podcast. Although Hebrew University subsequently rehired her, she was soon arrested and repeatedly questioned by Israeli police about her academic work and views. Furthermore, the Israeli Student Union has campaigned against her and other professors, proposing legislation aimed at limiting academic freedoms, including criteria by which an academic institution would be obligated to fire a faculty member.[64]

On May 5, 2024, Al Jazeera's East Jerusalem office was closed, its equipment confiscated, and access to its website blocked[65] . These measures were taken under a law passed by the Knesset on April 1, 2024, which **allows sanctions to be imposed on foreign broadcasters** in Israel.

4. Self-censorship as a measure of protection:

Using indirect measures to create a state of self-censorship that prevents Palestinians from freely sharing their opinions on social media platforms. These measures include firing from the workplace, dismissal from education, smear campaigns and hate speech, imposing financial restrictions on organizations active in the field of human rights, making bureaucratic procedures difficult, imposing unfounded administrative challenges, and making livelihoods contingent on not exercising the right to freedom of expression.

"This kind of practice creates great pressure on individuals and organizations and creates a kind of self-censorship. This is confirmed by a recent report issued by a campaign that stated that 60% of people in the West Bank, including Jerusalem, and 70% of people inside the West Bank have become self-censors, so that they refrain from publishing any content that may put them at risk (...) All media outlets have changed their publication standards (Editorial Policy) in the past years to adapt to the current situation. All media outlets have changed their Editorial Policy in recent years to adapt to the current situation. The editorial director of a media organization reported that in certain cases he fires an employee who publishes posts using language considered "inflammatory" by the platforms, justifying that this harms the organization in general and may lead to its closure." "Tagging police or Israeli authorities on social media posts that support trends contrary to occupation policy".[66]

[63] In a formal letter, the Education Minister directed schools to "immediately suspend any student or employee who supports the barbaric terrorist acts currently experienced in the State of Israel", and that, "In cases where there is indeed incitement, [you must] order a permanent expulsion." The letter issued by the Minister of Education is available in Hebrew at: https://bit.ly/48cYvq4 .

[64] 972 magazine, The orchestrated persecution of Nadera Shalhoub-Kevorkian Available at: https://bit.ly/4hi3lXh April 30, 2024

[65] 'Israeli Authorities Raid Al Jazeera After Shutdown Order' Reuters (Jerusalem/Doha, 5 May 2024) Available at: https://bit.ly/3Y4uh3J

[66] On September 16, 2024, a conceptual meeting (focus group) was held with various Palestinian civil society organizations to explore the Palestinian digital rights landscape between October 7, 2023 and September 1, 2024. The meeting was attended by the Arab Center for Community Media Development (7amleh), Human Rights Watch, Al-Haq, the Independent Commission for Human Rights, the Jerusalem Center for Legal Aid, and MIFTAH.

5. Content control on social media platforms:

Agreement with social media companies, especially META, **to block accounts, manage content, and impose high censorship on Palestinian content**, unlike Israeli content that contains direct inflammatory rhetoric against Palestinians, which is preserved and not blocked or removed. According to the HRW representative, “Meta has an entity that monitors accounts and manages Palestinian content. In contrast, Meta does not have a similar role for Israeli content,” **the HRW** representative said.From the beginning of the war until September 23, 2024, 5,456 cases of violations of Palestinian content[67] were documented. This figure does not reflect reality, only the cases that have been documented.

6. Smear campaigns against human rights defenders and supporters of the Palestinian cause.

Human rights defenders and supporters of the Palestinian cause are subjected to deliberate incitement and smear campaigns; during the period from the beginning of Israel’s assault on the Gaza Strip on October 7th, 2024, until September 23rd, 2024, 2,901 cases of incitement against Palestinians were recorded, including many cases against human rights defenders.

Regarding smear campaigns, there are many parties that work systematically to discredit individuals and institutions working in the field of human rights and advocating for the rights of Palestinians, the most important of which is **NGO Monitor**, a Jerusalem-based NGO that analyzes the work of international NGOs from a pro-Israeli perspective. **NGO Monitor** is described as a right-wing pro-Israel organization. **NGO Monitor** claims to have been founded to promote accountability and encourage active debate about the reports and activities of humanitarian NGOs in the context of the Arab-Israeli conflict. The organization was founded in 2001 by **Gerald M. Steinberg** under the auspices of the Jerusalem Center for Public Affairs and became a legally and financially independent organization in 2007.[68]

This organization monitors the performance of institutions and individuals who advocate for human rights and labels their performance “terrorist” or “anti-Semitic.” The organization considers cutting funding to human rights organizations and human rights defenders to be its main goal and one of its most important achievements. Another goal is to demonize anyone who advocates for the Palestinian cause and isolate them from credible international institutions and official international forums.

Palestinian civil society organizations have reported that the activities of the NGO Monitor group, which gathers the personal information of activists in the field from their social media accounts, have had a significant impact. The organization exerts pressure on foreign institutions and press; for example, the British newspaper The Telegraph published photos and information about former employees of the Campaign Foundation, describing them as anti-Semitic and terrorist, which has significantly damaged the organization's image abroad. Incitement against an organization ends with the closure of the organization as a whole.

Such attacks have compelled organizations to scrutinize what they publish carefully. Individuals have been harmed personally. For example, a human rights defender was prevented from obtaining a permit to visit and support one of his family members while he was receiving treatment in Jerusalem because of his work for one of the organizations that was subjected to a smear campaign through this platform.

[67]Sada Social Platform, available on: https://sada.social/ar

[68]Wikipedia (the free encyclopedia), NGO Monitor. Available from: NGO Monitor - Wikipedia (wikipedia.org).

Civil society organizations have reported that smear campaigns aim to destroy them or cut off their funding. In one instance, a pro-Israel organization conducted a smear campaign in which they portrayed six Palestinian organizations as supporters of by embellishing selected social media parts, with the result that they faced punitive measures[69] . This infringed the right of these organizations to conduct their activities to oppose the occupation and support human rights. In the same context, when organizations working at the Human Rights Council conduct activities with other organizations or countries, reports are prepared about their work, which is a violation of the Human Rights Council's own internal rules of procedure.

Philippe Lazzarini, Commissioner of the United Nations Relief and Works Agency for Palestine Refugees (UNRWA) expressed in a speech that was posted on X that he was “dismayed by the smear campaigns targeting Palestinians and those who provide them with aid[70].”

The Israeli occupation's **practices that limit freedom of expression** represent violations of international humanitarian and human rights law that amount to war crimes and crimes against humanity. Under the Fourth Geneva Convention, the occupying power – in this case, Israel – must respect the rights of civilians in the occupied territory, including their right to freedom of expression. These obligations go beyond mere passive protection, requiring the occupying power to take positive steps to ensure that the rights of the population are not violated. The evidence, however, indicates that Israel, through the illegal imposition of domestic law and military orders on the territory it occupies, is violating this obligation. For example, the administrative detentions systematically used in East Jerusalem and the West Bank show blatant disregard for Article 27 of the Convention, which obligates the occupying power to protect the rights of the civilian population. These detentions, carried out without due process, show a lack of respect for the international standards that prohibit arbitrary detention. In addition, they have a neutralizing effect on civil society, as individuals are afraid to express their opinions or participate in political activities, negatively impacting the community's ability to exercise its rights.

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) sets a clear standard for the protection of freedom of expression. This right requires special protection from the state, which means that authorities must avoid any arbitrary or retaliatory actions against individuals for their opinions or expressions. Arrests made under Israel's 2016 anti-terrorism law show how national laws can be used as a tool to justify abuses. These laws are often ambiguous in their definition of “incitement,” giving authorities broad license in their enforcement. This demonstrates an inability to adhere to the standards of international law, which state that in a democratic society any restrictions on freedom of expression must be clearly justified as necessary. In this context, it must be highlighted how these policies affect Palestinian society, with many individuals expressing fear of expressing their opinions, leading to an environment of self-censorship. These dynamics point to the urgent need to reassess domestic law and ensure their compatibility with the state's obligations under international human rights law.

From the perspective of international criminal law, the Rome Statute, particularly Article 7, highlights that the arbitrary and systematic detention of civilians is considered a crime against humanity. This article is crucial in determining criminal responsibility for human rights violations, as it allows the international community to take legal action against individuals who implement or legitimize such policies[71].

[69] Adalah, Israel's declaration of 6 Palestinian human rights groups as ‘terrorist organizations’ 30/12/2021, Available at https://bit.ly/3Y3qC6j
[70] Anadolu Agency, UNRWA expresses "appallment over defamation of Palestinians", 12/17/2023, available at: https://bit.ly/3YnWpjy
[71] UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), ISBN No. 92-9227-227-6, UN General Assembly, 17 July 1998. Article 7 (1) (E).

In the current situation in Palestine the systematic targeting of Palestinians by Israel because of their views constitutes a crime against humanity. Arrests of Palestinians by Israel on vague and imprecise charges emphasize the need for an independent international investigation to document violations and identify perpetrators. Israel's lack of accountability for these violations encourages their continuation and contributes to a culture of impunity. Therefore, enhanced cooperation between states and human rights organizations is needed to ensure that the individuals involved in these violations are held accountable. Achieving justice and accountability is essential not only for victims, but also for the preservation of the international human rights-based order.

Restrictions on the Right to Privacy

The right to privacy is a fundamental digital right in the modern era, gaining increasing importance as the use of technology and the Internet expands exponentially. This right requires that individuals' personal data be protected and prevented from being exploited or violated by governments, companies, or other individuals. In the digital context, privacy includes the protection of the personal information that is collected, stored, and processed through digital platforms, as well as ensuring the confidentiality of electronic communications and correspondence. Preserving this right is essential to achieving a safe and open digital environment in which human rights are respected, especially in light of the development of tracking and surveillance technologies that may threaten the privacy of individuals and expose them to serious violations.

In the Palestinian context, the hacking of personal information is not only a violation of the right to privacy but is also used by Israel as a tool to identify individuals as military targets by monitoring of their mobile devices, correspondence, and social media interactions.

The Israeli occupation employs numerous practices that invade the privacy of Palestinians in the occupied territories. In East Jerusalem, Israel illegally applies domestic policies that are at odds with international standards for protecting the right to privacy (as explained previously); in the West Bank and Gaza, military orders are issued that violate the rights of Palestinians to privacy.

In fact, the Israeli occupation does not need any law or justification to hack into Palestinian information. As it is Israel that provides the Palestinians with the technology needed to provide telecommunications services in the West Bank and Gaza Strip. Therefore, all information that travels through the granted frequencies and waves is directly hacked by the occupation.

Israel's violations of Palestinians' right to privacy fall into two main categories:

1. Seizing of electronic devices of Palestinians in public places and at checkpoints, harvesting information from the devices, and social loopholes to use the information obtained to blackmail individuals based on this information[72].
2. Penetrating the Palestinian telecommunications sector completely. An expert in the field of telecommunications emphasized that Israel has free access to the data on the mobile phones of Palestinians in the West Bank and Gaza Strip because it is the one who gives them the technology and controls the frequencies used by mobile network operators in the occupied territories.

[72] 7amleh - Arab Center for the Development of Social Media, Study on Digital Security among Palestinian Youth in the Shadow of the War on Gaza, 8/20/2024 Available at: https://bit.ly/486c5ve

Article 29 of the Palestinian Basic Law guarantees the freedom of the press and the media and recognizes the right of any individual to establish a newspaper or media house and to print, publish, distribute and transmit. It prohibits the imposition of any form censorship on the media, including warnings, suspension, confiscation, cancellation, or other restrictions, except in accordance with legal provisions and judicial authorization, thereby promoting the right to access to information. In addition, Article 6 of the Basic Law stipulates that official bodies must facilitate the task of journalists and researchers in accessing their programs and projects, which increases the effectiveness of oversight and accountability. Despite these guarantees, the Basic Law lacks explicit provisions guaranteeing freedom of access to information. This constitutes a loophole that may be used to limit access to information.

6. Israeli Digital Tools: Their Concept and Types

The use of digital tools based on data interceptions was used by Israeli to achieve unlawful military objectives. In May 2024, Human Rights Watch discovered data that Israeli military had posted publicly online – apparently in error – embedded in the source code of the Evacuation Information website of the Israeli Defense Force (IDF). The data included what appeared to be operational data related to the systems used by the Israeli military to monitor the evacuation and movement of people across Gaza, as well as to assess the potential harm to Palestinian civilians that might result from attacks planned by the Israeli military. The data also included the personal information of residents of Gaza and the names of the most populous extended families in each bloc. The data contained population figures consistent with Gaza's ten-year census data, disaggregated population data, information about civilian population movements and Israel's military presence in Gaza, and the cumulative number of attacks made on each of the 620 blocks that make up the Gaza Strip. The data also included personal information: The surnames of the largest families in each part[73].

Documentation indicates that the Israeli military has used four broad types of tools that rely on digital technology in its assault on Gaza. These tools are used for a range of purposes, including monitoring population movement, assessing targets, and timing attacks. The types of tools are as follows:

1. Evacuation monitoring tools. These rely on cellphone tracking to monitor civilian movements in northern Gaza and identify evacuation zones[74].

2. The Gospel AI system. This is used to prepare lists of structural targets, such as buildings and public facilities. The Gospel uses an algorithm to process surveillance data in order to generate target lists. Based on media reports, the Gospel identifies four categories of non-human targets: military targets, including underground targets, such as tunnels, and the family homes of suspected militants, and ‘force targets’, which are civilian structures that are attacked with the stated goal, according to current and former intelligence analysts quoted in media reports, of “creating a shock” that would “push civilians to pressure Hamas.” Articles posted on the IDF website in 2022 and 2023 described a tool based on a Gospel-like algorithm, some of which mentioned it by name.[75]

3. Lavender AI-assisted system. This tool uses machine learning to categorize people based on their degree of association with armed groups. Israel uses Lavender to give Palestinians in Gaza a numerical score. According to reports, IDF officials reportedly set the threshold beyond which a person can be categorized as an attackable target.[76]

[73] Ibid.

[74]- Human Rights Watch. “Q&A: The Use of Digital Tools by the Israeli Army in Gaza”. Published in 10 September 2024. Check the link: http://tiny.cc/feu4001

[75] The Guardian, ‘The Gospel’: how Israel uses AI to select bombing targets in Gaza, 1 Dec 2023. Available at: https://bit.ly/3zY8rqE ts

[76]- Human Rights Watch. “Q&A: The Use of Digital Tools by the Israeli Army in Gaza”. Published in 10 September 2024. Check the link: http://tiny.cc/feu4001

4. Where's Daddy? AID system. This is used to determine the most appropriate time and location to attack a particular target. Detailed information about its development is not available.[77]

International humanitarian law requires the parties to a conflict to distinguish between civilian and military targets and to take all precautions to minimize harm to civilians.However, relying on inaccurate data such as that collected from cellphones puts civilians at serious risk. For example, Israel's evacuation monitoring tool relies on cellphone 'triangulation' to determine the approximate location of people, a technology that is not precise enough to make accurate military decisions.

Lavender relies on machine learning techniques that collect and analyze data from unlabeled sources to determine whether someone is a threat. However, this type of technology depends on unproven assumptions, and the data can be incomplete or biased[78]. This directly affects the accuracy of target categorization as well as the legality of attacks based on these categorizations.[79]

International Humanitarian Law (IHL) constitutes a significant part of the legal foundations for the of protection of individuals during armed conflicts and focuses on protecting civilians from harm in the context of a conflict. Although IHL does not address the right to privacy explicitly, many of its general principles – such as the principle of distinction between civilians and combatants and the principle of proportionality in the use of military force – establish the protection of privacy as an integral part of human dignity and fundamental rights[80].

In armed conflict, civilians are protected from unlawful targeting, including unwarranted interference with their private lives. For example, individuals' personal data and freedom of communication must remain protected from any unwarranted infringement. Digital espionage and mass surveillance targeting civilians without distinguishing between individual civilians and combatants violates the fundamental principle of distinction, which is the cornerstone of the protection of civilians under IHL.

According to the IHL principle of proportionality, any military action taken must be proportionate to the military objective pursued and must not result in unjustified civilian casualties or violations of their fundamental rights. However, the indiscriminate use of sophisticated digital tools used in Gaza, such as AI-assisted systems The Gospel and lavender, violate this principle. These tools allow Israeli military forces to collect unlimited amounts of personal data on civilians without their consent, putting them at risk of direct targeting or discrimination based on inaccurate or misleading personal information.[81]

The "Where's Daddy?" AI-assisted system, which is used to locate potential attack sites based on personal data analytics, violate the principle of proportionality because relying on inaccurate data can lead to disproportionate targeting and harm to civilians, contrary to international obligations to protect civilians[82].

[77]- Ibid

[78] Antonio Coco, Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes, Journal of International Criminal Justice, Volume 21, Issue 5, November 2023, Pages 1077–1096, https://doi.org/10.1093/jicj/mqad034

[79]- Human Rights Watch. "Q&A: The Use of Digital Tools by the Israeli Army in Gaza". Published in 10 September 2024. Check the link: http://tiny.cc/feu4001

[80] Additional Protocol to the Geneva Conventions of August 12, 1949 (Protocol I), Articles 51(5)(b) and 52(2); The Hague Convention (II) on the Laws and Customs of War on Land (1899); Introduction. Rome Statute of the International Criminal Court, Article 8(2)(b)(iv); International Committee of the Red Cross, Customary International Humanitarian Law, Rule 14.

[81]- Human Rights Watch. "Q&A: The Use of Digital Tools by the Israeli Army in Gaza". Published in 10 September 2024. Check the link: http://tiny.cc/feu4001

[82]- Ibid

Military authorities often justify the violation of civilian privacy during armed conflicts on the pretext of 'military necessity'. However, according to international humanitarian law, such military measures must be strictly regulated and may not exceed military necessity. In other words, belligerent forces can only violate the rights of individuals, including their privacy, if it is necessary to achieve a legitimate and proportionate military objective[83].

The widespread collection of digital data without individual consent or impartial oversight, as is happening in Gaza, is inconsistent with these principles, especially given the evidence that this data is being used to commit international and retaliatory crimes and expose civilians to further harm without a compelling military justification.

An important aspect in this context is the relationship between privacy and human dignity, which is a fundamental issue in both international humanitarian law and international human rights law.[84] Violating the digital privacy of civilians, whether by spying on their communications or monitoring their daily online activities, is a gross violation of their human dignity. These violations pose a serious threat to the psychological and physical integrity of individuals who must be protected under the law.

While international humanitarian law provides for the protection of civilians during armed conflicts, international human rights law plays an important role in promoting the right to privacy at all times, whether in times of peace or war. In this context, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) guarantees the protection of individuals from arbitrary or unlawful interference with their privacy, family, or correspondence. In armed conflicts, such as the current conflict in Gaza, this protection is particularly important, as privacy is vulnerable to systematic violations, whether by warring parties or external actors.

Although international humanitarian law focuses on protecting civilians in wartime, this does not mean that basic human rights cease during conflicts. In fact, the International Committee of the Red Cross (ICRC) emphasizes that international human rights law continues to apply in wartime, meaning that the right to privacy remains largely protected even during armed conflicts.

Israel's gathering of the personal data of Palestinians without consent – whether manually or remotely – in Gaza and the West Bank, and use of this data to identify military targets, are violations of both international humanitarian law and international human rights law. Stringent measures are needed to ensure Israel's compliance with these international standards and strengthen the protection of the privacy of Palestinians in territory occupied by Israel.

[83] 1977 Additional Protocol I to the Geneva Conventions, Article 48.

[84] international Covenant on Civil and Political Rights, Article 17. Geneva Conventions, Common Article 3. Human Rights Committee, General Comment No. 16 (1988) on the right to respect for privacy. United Nations Human Rights Council, Resolution on the promotion and protection of human rights in the context of human security (A/HRC/RES/24/30).

7. The Collusion of Global Corporations with the Israeli Occupation

In the context of the Israeli occupation of Palestine, the involvement of multinational corporations raises significant concerns regarding their complicity in human rights violations and breaches of international law. This section explores the role of some of the world's largest technology companies—including Meta, Alphabet (Google), Amazon, and others—in facilitating and sustaining the Israeli occupation through practices that undermine Palestinian rights and freedoms.

Through digital censorship, surveillance technologies, and misrepresentation of facts, these corporations contribute to the marginalization of Palestinian voices and the perpetuation of oppressive policies. Moreover, the alignment of corporate operations with the strategic interests of the Israeli military and government exacerbates the violations faced by Palestinians in occupied Palestine. The following analysis delves into the specific roles and actions of these corporations, shedding light on how their policies and technologies intersect with systemic human rights abuses in Palestine, and calls for greater corporate responsibility in the face of global injustice.

1. Meta

Since the beginning of Israel's current assault on Gaza, the censorship and suppression of Palestinian and pro-Palestinian voices on social media platforms has escalated substantially – most notably on Meta. This wave of censorship, which coincides with the ongoing violence in Gaza and international warnings of genocide, perpetuates Meta's long history of systematic censorship of content related to Palestine. Despite the company's statement that it does not seek to "suppress a particular community or point of view", documentation of Meta's censorship on the platform suggests otherwise. Meta has contributed to managing Palestinian content and destabilizing the Palestinian narrative through several measures that have been applied in a way that violates Palestinian human rights and discriminates in the treatment of users.

As Israel began bombing the Gaza Strip in October 2023, Palestinians and pro-Palestine advocates began to complain about censorship on Meta's platforms, such as Facebook and Instagram. This censorship included suspending or restricting the accounts of journalists and activists inside and outside of Gaza and removing large amounts of content documenting human rights violations and atrocities.

Examples based on testimonies and documentation show that censorship is systematic and global. For example, Human Rights Watch documented 1,049 removals of peaceful content expressing support for Palestine from more than 60 countries between October and November 2023. The Palestinian Observatory for Digital Rights Violations recorded 1,043 cases of censorship between October 7th, 2023, and February 9th, 2024, on **Facebook and Instagram.**[85]

Patterns that have been documented include arbitrary content deletions, vague account restrictions, and the use of **shadow-banning**, which is the process of restricting access to user content without informing the user. Perhaps one of the most well-known instances of this is the experience of Mohammed al-Kurd, a prominent Palestinian writer and activist. during the May 2021 uprising. Al-Kurd regularly received more than 150,000 views on his stories, but when he started posting about the eviction of his family in the Sheikh Jarrah neighborhood of East Jerusalem, his story views dropped to a much lower number[86]. Many Palestinians have reported similar experiences when they post about Palestine. In this way, **shadow banning** silences Palestinians who are trying to share their voices, perspectives, and lives. Social media platforms do not tell users that they are being shadow-blocked.

[85] Human Rights Watch Report, Meta's Broken Promises, December 21, 2023. Available at: https://bit.ly/403Hcph

[86] 7amleh- The Arab Center For the Advancement of Social Media, Meta, let Palestine Speak Campaign Q&A. Available at:https://bit.ly/3Y7Woz9

Human rights organizations including the **7amleh Center for Community Media Development, Human Rights Watch, and Access Now** have identified six common practices used by social media platforms in this pattern of unjustified censorship. These include[87]:

- **removal of posts, stories, and comments;**
- **suspension or permanently disabled accounts;**
- **temporarily restricting users' ability to interact with content** – such as liking, commenting, sharing, and reposting – for periods ranging from 24 hours to 3 months;
- **restricting users' ability to follow or tag other accounts;**
- **restricting access to the use of certain features, such as Instagram/Facebook live**, monetization, and recommending accounts; and
- **"shadow banning,"** a significant reduction in the visibility of content without prior notice.[88]

Human Rights Watch has identified **four key factors** that have contributed to this pattern of censorship[89]:

a. Weaknesses in Meta's policies, especially the 'Dangerous Organizations and Individuals' (DOI) policy, which relies on vague lists and broad definitions.
b. The inconsistent and non-transparent application of Meta's policies, especially with regard to news content that is supposed to be exempted in the public interest. In this context, Hamama and **Human Rights Watch** confirmed the presence of a monitor on Palestinian content in Arabic and the absence of a monitor on Israeli content in Hebrew, which led to a rise in hate speech and incitement against Palestinians by settlers and the Israeli government, with more than 2900 instances of inflammatory content against Palestinians documented during the recent war on the Gaza Strip[90].
c. Responding to government pressure, such as requests from the Israeli Cyber Unit to remove content.
d. Over-reliance on automated tools to remove Palestine-related content.

Through these policies, Meta directly restricts Palestinians' right to freedom of expression and unjustifiably violates the privacy of individuals in contravention of international human rights law.

Thus, the freedom of expression of Palestinians is currently facing significant barriers as a result of the collaboration of Meta with the Israeli occupation forces, at a time when this right is one of the most widely recognized human and digital rights and is explicitly guaranteed under international human rights and humanitarian law.

In addition, the United Nations Guiding Principles on Business and Human Rights make it clear that businesses should respect human rights. The Guiding Principles state: "Business enterprises should avoid violating human rights and address any negative impacts that may result from their activities[91]."

The Principles also indicate that corporate responsibility to respect human rights is based on internationally recognized rights. Based on these international legal principles and the substantial evidence of the systematic censorship and silencing of Palestinian voices on Meta's platforms, it is clear that Meta is violating international law. Meta has also run advertisements promoting land development in Israel's illegal settlements[92] that are spread across the occupied West Bank and East Jerusalem.

---

[87]- 7amleh, "What is Meta, and why are they important to Palestinian digital rights?". Check the following link: https://meta.7amleh.org/Q&A
[89]- Human Rights Watch. "Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook". Published in December 21, 2023. Check the following link: http://tiny.cc/ju35001
[90] The Sada Social platform, available on: https://sada.social/ar
[91]UN Guiding Principles for Business and Human Rights. Namely principles 11-14.
[92] 7amleh- The Arab Center For the Advancement of Social Media, Meta, let Palestine Speak Campaign Q&A. Available at: https://meta.7amleh.org/Q&A

The construction and existence of these settlements violate Article 49 of the Fourth Geneva Convention and constitute a war crime amounting to a crime against humanity according to the Rome Statute of the International Criminal Court[93].

2. Alphabet

Google's parent company, Alphabet, contributes to the Israeli government's violation of international human rights and humanitarian law through numerous practices that constitute war crimes. These include:

a. Project Nimbus, in partnership with Amazon

The $1.2 billion Nimbus project is designed to provide cloud computing services to the Israeli military and government, enabling them to increase surveillance capabilities, illegally collect data on Palestinians, and facilitate the expansion of illegal settlements on occupied Palestinian land.[94]

The project is being implemented through several phases. The first begins with the procurement and establishment of the cloud infrastructure, followed by the formulation of a government policy to move operations to the cloud, followed by the actual migration of operations to the cloud platform, and finally, implementing and optimizing those cloud processes.[95]

Google Cloud Platform and Amazon Web Services have been selected to provide the agencies of the Israeli occupation authority with cloud computing services, including artificial intelligence and machine learning technology, according to a report from the Jerusalem Post. These services are being used to expand settlements by supporting the data of the so-called ‘Israel Land Administration’, as well as enhancing the surveillance systems used against Palestinians in the West Bank, increasing human rights violations and displacement of the Palestinian population.[96]

The Israeli military relies heavily on advanced data-driven surveillance systems. With the augmentation of these systems by Google's technologies, military repression is expected to be exacerbated. Some Google engineers have expressed concern that employees are not privy to the details of the project, citing the use of this technology to oppress Palestinians as a major concern.

According to leaked training documents, Google provides the occupation government with a wide range of AI and machine learning tools through its cloud platform, giving Israel capabilities such as face detection, automated image classification, object tracking, and sentiment analysis – technologies that are controversial due to growing doubts about their reliability and effectiveness.

[93]Rome statute, articles 7, 8.

[94] Aljazeera - What is Project Nimbus, and why are Google workers protesting Israel deal? 23, Apr, 2024. Available at: https://bit.ly/4dSQ1FS

[95]Aljazeera - What is Project Nimbus, and why are Google workers protesting Israel deal? 23, Apr, 2024. Available at: bit.ly/4dSQ1FS

[96] The Times of Israel. Israel signs deal for cloud services with Google, Amazon, 24 May 2021. Available at: https://bit.ly/401Xkra and The Guardian, We are Google and Amazon workers. We condemn Project Nimbus, We cannot support our employer’s decision to supply the Israeli military and government technology that is used to harm Palestinians. 12 Oct 2021 https://bit.ly/3Y31D2Y

b. Google Maps

As one of the world's leading technology companies, Google is one of the most influential providers of geographic services through its Google Maps service, which is used by millions of people around the world on a daily basis. However, Google's presentation of a map of Palestine raises many questions about the company's compliance with international law, especially in the context of the Israeli-Palestinian conflict. In terms of Google's misrepresentation of the region and the legal implications according to the standards of international law, there are several issues:

1. **Failure to name Palestine as a recognized state:** Despite a 2012 UN General Assembly resolution (Resolution 67/19) recognizing Palestine as a non-member observer state, Google does not show the 'State of Palestine' on its maps, instead showing Palestinian areas fragmented within Israel's borders.
2. **Displaying Jerusalem as the capital of Israel:** Google presents Jerusalem as the unified capital of Israel without reference to its disputed status. UN General Assembly Resolution 181 states that Jerusalem falls under international status (Corpus Separatum); it thus cannot be unilaterally declared the capital of Israel.
3. **Exclusion or limited inclusion of Palestinian villages, especially in Area C:** Palestinian villages in Area C, which is under full Israeli control, are either not shown on the map or are presented in limited detail compared to Israeli settlements. This includes those Palestinian villages that the Israeli authorities refuse to recognize despite their actual existence.
4. **Illegal Israeli settlements are not highlighted:** Israeli settlements in the West Bank are displayed in the same way as other Israeli cities on Google Maps. These settlements are illegal according to international law, especially Article 49 of the Fourth Geneva Convention and Article 55 of the Hague Regulations.
5. **Failure to indicate the divisions of the West Bank areas (A, B, and C):** Google does not distinguish between the West Bank areas (A, B, and C) as agreed upon in the Oslo Accords, engendering confusion about the legal and administrative boundaries of the different areas.
6. **Failure to display movement restrictions:** Military checkpoints, restricted access to streets or areas, and other geographical spaces that are specially restricted to Palestinians are adequately represented, with the result that the geographical landscape that Palestinians live in under Israeli occupation is not accurately represented.
7. **Changing or omitting Palestinian historical names:** Google Maps has assigned Israeli names to some Palestinian areas and streets, contributing to the erasure of Palestinian historical and local names (e.g. changing the name of Jerusalem Street).

Google Maps' misrepresentation of Palestine as breaches of international law

1. **Failure to recognize Palestine as a state:** As the United Nations recognized Palestine as a state in 2012, Google Maps' exclusion of the name 'State of Palestine' from its maps disregards this international recognition. This undermines Palestine's legal status in accordance with the international resolution and affects the Palestinians' right to self-determination, a fundamental principle of international law as enshrined in Article 1 of the UN Charter and the International Covenant on Civil and Political Rights (ICCPR).
2. **Misrepresentation of Jerusalem:** Google's presentation of Jerusalem as Israel's unified capital contradicts UN General Assembly Resolution 181, which establishes a special international status for the city. Google's alignment with Israel's unilateral declaration of Jerusalem as its capital violates the principle of non-recognition of the acquisition of territory by force, as enshrined in the UN Charter Article 2(4).

3. **Exclusion of Palestinian villages in Area C:** Area C is part of the West Bank under full Israeli control and includes many Palestinian villages. The exclusion of these villages from Google Maps supports Israeli policies aimed at marginalizing the Palestinian presence in these areas, which can be considered a violation of international humanitarian law, especially Article (43) of the Hague Regulations, which obliges the occupying power to respect local laws in the occupied territories.
4. **Failure to note the illegal nature of settlements:** Israeli settlements in the West Bank are illegal under Article 49 of the Fourth Geneva Convention, which prohibits the transfer of the occupying power's civilian population into the occupied territory. By not classifying these settlements as illegal, Google is contributing to the normalization of Israeli settlement activities, ignoring international law, including UN Security Council Resolution 2334, which affirms that Israeli settlements are illegal.
5. **Failure to delineate areas A, B, and C:** The Oslo Accords divided the West Bank into Areas A, B, and C, each with a different level of Palestinian and Israeli control. The failure to delineate these areas on Google Maps ignores international agreements and undermines an accurate legal and practical understanding of the situation on the ground.
6. **Omission of movement restrictions:** Israeli authorities impose severe restrictions on Palestinians' freedom of movement, including checkpoints and prohibiting access to roads or areas. Failure to represent these restrictions in Google Maps ignores the right to freedom of movement, a right protected under international human rights law and Article 12 of the International Covenant on Civil and Political Rights (ICCPR).
7. **Erasing Palestinian names:** Changing or omitting Palestinian names on Google Maps contributes to the erasure of the cultural and historical heritage of Palestinians, which is a violation of international conventions on the protection of cultural heritage and the right of peoples to preserve their cultural identity as stipulated in the preamble of the International Covenant on Economic, Social and Cultural Rights (ICESCR).

Google Maps' representation of Palestine, including not recognizing the State of Palestine, changing the status of Jerusalem, and omitting illegal settlements, is a clear violation of the standards of international law. These practices contribute to the marginalization of the Palestinian state and the normalization of the Israeli occupation. According to the UN Guiding Principles on Business and Human Rights, Google, as a company, has a responsibility not to contribute to human rights violations and to ensure that its practices are consistent with international law.

c. Amazon, Microsoft, Google, Oracle, and IBM

These companies contract directly with US intelligence agencies and the Department of Defense, which provides material support and intelligence to the Israeli government on an ongoing basis and, particularly, for its current assault against Gaza.

Reports indicate that Microsoft has a $22 billion contract with the US military to supply the Integrated Visual Augmentation System from March 2021 to March 2031.Amazon contracted with the US National Security Agency for $10 billion to supply Wide and Stormy, and Amazon, Microsoft, Google, Oracle, and IBM contracted with the CIA and the US Department of Defense to supply cloud software worth tens of billions of dollars[97].

[97] Roberto J. González, "How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex," (San José State University, April 17, 2024).

Companies have a responsibility to refrain from violating human rights under either International Humanitarian Law (IHL) or International Human Rights Law (IHRL). These two legal frameworks aim to protect individuals from serious violations, especially in times of armed conflict and war, but they also apply in normal circumstances. Therefore, companies' adherence to these standards not only depends on local laws in the countries in which they operate but must be in line with recognized international standards.

According to the United Nations Guiding Principles on Business and Human Rights (UNGPs), adopted in 2011, companies have a responsibility to respect human rights at all stages of their operations. These principles – particularly, Principles 11, 13, and 17 – are based on the international human rights framework and clarify the responsibility of companies in preventing human rights violations.

Principle 11: Responsibility to refrain from infringing on human rights

Principle 11 states that companies should respect human rights and not contribute to their violation, regardless of their size or industry. This requires companies to take practical measures to ensure that they do not contribute, directly or indirectly, to human rights abuses, either through their operations or through their supply chain.

Principle 13: Responsibility to institute preventative measures

Principle 13 outlines the need for companies to take effective action to prevent adverse human rights impacts associated with their activities or operations. This includes the obligation to assess the risks surrounding their business and environment, and to take practical measures to minimize and address these risks if they occur.

Principle 17: Human rights due diligence

According to Principle 17, companies should conduct a human rights ‘due diligence’ process by identifying, preventing, and mitigating any negative impact on human rights that may arise from their business. This process includes steps to assess the impact, identify areas most vulnerable to violations, and take measures to rectify the damage.

Based on the UN Guiding Principles and international law, companies are required to adopt policies and procedures that ensure their full compliance with human rights. Failure to do so may lead to corporate accountability, especially if they contribute to serious violations such as war crimes or repeated human rights violations.

8. Practices of the Palestinian National Authority

As the reliance on digital technology expands in all areas of contemporary life, safeguarding the digital rights of individuals has become one of the main challenges facing states and societies. In the Palestinian context, the issue of digital rights is even more complex given the political and security situation faced by the Palestinian National Authority (PNA). Although Palestine has acceded to several international conventions that guarantee human rights[98], including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, since 2014[99], the actual implementation of these international obligations faces increasing difficulties on the ground.

The Palestinian territories are subjected to a wide range of practices that constitute violations of digital rights – ranging from restriction on freedom of expression online to surveillance of personal data and censorship on social media. These violations are committed not only by the Israeli occupation authority but also by the PNA, which has been found to exploit the broad and ambiguous language of some legislation to impose restrictions on digital freedoms. This raises questions about the Palestine National Authority's commitment to protecting these rights and prompts a careful analysis of the national and international legal framework that should govern this issue.

In terms of the Palestinian legal framework that aims to protect the digital rights of individuals, the Palestinian Basic Law (amended in 2003) is the main pillar that guarantees individual freedoms and rights. Article 19 of the Basic Law guarantees freedom of opinion and expression, and Article 27 protects the freedom of the media. These provisions reflect a theoretical commitment by the Palestinian Authority to preserve the rights of citizens to express their opinions and access information.

However, other laws appear to complicate the situation and open the door to restrictions of these rights. For example: Cybercrime Law No. 10 of 2018, which was designed to combat cybercrime and protect individuals from digital threats, has become one of the most controversial laws in the Palestinian context, because it contains text that can be used to suppress freedom of expression online. Article 39 of the law gives authorities the power to block websites based on threats to national security, public order, or public morals, but no criteria are provided for determining what qualifies as a threat, creating leeway for the law to be used to abuse freedoms.

In addition, other laws, such as the Press and Publication Law No. 9 of 1995, reinforce some rights, but do not provide adequate protection in the context of today's digital world, creating a significant legal gap that needs to be addressed. Despite Palestine's accession to the International Covenant on Civil and Political Rights, which guarantees in Article 19 the right of everyone to freedom of expression and to receive and impart information without interference, the practical application of this right faces challenges within the Palestinian legal system due to local laws that sometimes conflict with international standards.

[98] Maqam - Encyclopedia of Palestinian laws and court rulings. International conventions, treaties and covenants to which Palestine has acceded, available at https://bit.ly/4dJiRZ4

[99] United Nations Human rights, Office of the High Commissioner, Status of Ratification Interactive Dashboard https://bit.ly/4dQktAe , Accessed 15, Sep, 2024

An analysis of Palestinian law related to digital rights exposes a clear contradiction between the commitments made by the Palestinian Authority to international treaties and its actual practices on the ground. While domestic legislation, such as the Basic Law, includes provisions that promote freedom of expression and privacy, other laws, such as the Cybercrime Law, allow the Authority to exercise broad powers to monitor digital activities and block content.

Even more troubling is the use of broad and undefined terms in these laws, such as “national security,” “public order,” and “public morals,” which can be interpreted in different ways depending on the political or security orientation of the authority. This legal ambiguity allows for practices that may arbitrarily violate the rights of individuals and leads to the curtailment of digital freedoms rather than protecting them. Article 45 of the Cybercrime Law adds another complication, as it allows for the imposition of penalties for acts that the law considers criminal without clear definition, raising concerns that this provision could be used to criminalize legitimate practices in the context of freedom of expression, such as expression of opinion or criticism.[100]

Regarding the right to privacy, although Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary interference with the privacy of individuals, Palestinian legislation has not provided sufficient regulation to protect digital privacy. Electronic surveillance, for example, is not clearly defined in the Basic Law or other laws, giving the authorities a wide margin to interfere in the personal lives of individuals without strict legal controls.

This analysis reveals gaps in the Palestinian legal framework that undermine the protection of digital rights. While some legal texts reflect Palestine's international obligations in this area, other laws, especially the Cybercrime Law, contradict these obligations and open the door to widespread violations. The biggest challenge lies in the lack of clarity of some legal texts and the ambiguity of terms such as ‘national security’ and ‘public order’, allowing them to be used as tools to restrict, rather than protect, digital freedoms.
Consequently, there is an urgent need to review and amend Palestinian legislation related to digital rights to ensure real protection of these rights and align them with international standards. These revisions must be clear and precise to ensure that the law is not exploited to restrict digital freedoms but rather serves to promote them and protect them from violations, whether by local authorities or other entities.

The role of the Palestinian National Authority in the protection of digital content

The Palestinian National Authority (PNA), as a state, has a crucial role to play in protecting citizens’ rights on the Internet, including their right to post content that documents human rights violations committed by the Israeli occupation forces.As these platforms have a history of bias in their handling of content related to Palestine, this means that in its duty to protect this right the PNA is required to communicate with social media platforms to prevent deletions or restrictions. However, the Authority does not have the necessary power to lobby these platforms to revise their policies. In addition, it has not demonstrated the political will to address these practices. On the contrary, the Authority has shown a tendency to remove content that criticizes its own policies. As a result, the right of Palestinians to post content regarding violations of rights by Israel and criticism of the Authority itself is not protect. In this matter, the Authority sees them as double opponents.

[100] Human Rights Watch Report, Meta’s Broken Promises, December 21, 2023. Available at: https://bit.ly/403Hcph

Social censorship and family influence: internal factors limiting freedom of expression

Instead of using its powers directly to silence individuals who use their freedom of expression to express views in ways that it opposes – which would enable documentation of such violations – the Palestinian Authority relies heavily on social and family pressure to influence individuals and limit their freedom of expression. The Authority has been found to pressure the families of individuals working in the government or who have family influence to pressure activists or critics. This may involve informing relatives working in the Authority of the movements or statements of family members, who then pressure the targeted person to remove the content or reduce its publication[101]. This type of pressure, which occurs informally and within the family, is difficult to document, making it a powerful and invisible tool to limit freedom of expression.

The impact of this type of pressure is magnified when it comes to women, as women in conservative societies such as Palestine are considered a vulnerable group. Women human rights defenders find themselves under additional social pressure, as the threat of being exposed or their reputations tarnished increases if they publish content that criticizes the Authority or objects to government policies.[102].

The use of deterrence and defamation policies to intimidate human rights defenders

The Palestinian Authority has followed a systematic policy of deterring human rights defenders through smear campaigns. In cases of large protests, such as those following the killing of activist Nizar Banat, the Authority has used personal photos of women activists as a tool to generate intimidation and fear. This tactic has led women to refrain from participating in demonstrations and public positions, for fear of being defamed or having their private lives exposed. This strategy has proven largely successful in reducing the number of women activists participating in the public space – an indication of the effectiveness of this deterrent policy in suppressing freedom of expression.

Other methods, such as limited arrest of protesters, defamation, and even blackmail, have been used to deter individuals from joining public protests or posting their opinions online, for fear of the repercussions they may face from their families or communities.

Organized security campaigns and digital intervention

The Palestinian security services have organized mass reporting campaigns against content that conflicts with their standards. These agencies monitor individuals' digital activity and use mass reporting techniques against content they deem inappropriate or critical of the authorities. These campaigns make it difficult for individuals to freely express their opinions, as any content that conflicts with the authorities exposes its author to the risk of deletion or restriction by social media platforms, thanks to the pressure exerted by these security campaigns[103].

[101] A consensus view of the civil society organizations represented in the focus group meeting (16 September 2024), op. cit.

[102] Ibid

[103] Report by Al-Araby Al-Jadeed platform - Targeting Palestinian content: Digital campaigns led by PA affiliates https://bit.ly/4f52TJZ

Weak political will and legal challenges

Although the Palestinian Authority has signed several international agreements that guarantee the protection of human rights, its commitment to implementing these agreements appears weak on the ground. The Palestinian Authority shows no interest in enacting or passing laws that may not serve its political strategies, such as the Family Law, and leaves many legal loopholes unaddressed. Failure to harmonize laws reinforces the violation of individuals' digital rights. It also allows the Cybercrime Law to be interpreted in a way that harms freedom of expression, as it is used to restrict critical content while it is not applied against groups that conduct smear campaigns against human rights defenders, such as the Anti-CEDAW Coalition.[104]

Blackmail and exploitation of social loopholes: an informal repressive system

Cyber blackmail, account theft, and identity theft are among the biggest challenges facing individuals in Palestine. With a lack of real political will on the part of the PA to deal with these issues, many victims resort to personal solutions to confront their attackers. At the same time, the PA and the Israeli occupation authorities use blackmail to pressure individuals into sensitive situations, especially when it comes to the most socially vulnerable individuals, such as homosexuals.[105]

In this context, the Israeli occupation's exploitation of these social gaps stands out, as individuals who are exposed to great social pressure are targeted, and this pressure is used as a tool to suppress them or force them to collaborate. This tactic is considered part of a systematic policy aimed at breaking the morale of individuals and societies by exploiting social weaknesses[106].

Role of Palestinian corporations in the breach of the right to privacy

Palestinian telecommunications companies play a pivotal role in facilitating violations of individuals' privacy and digital rights. Despite stating that they do not have the authority to access user content or record calls, there is evidence that these companies cooperate with security services to provide information about users, such as their IP addresses. The role of companies in blocking websites has also been documented; in 2017, for example, several websites were blocked on the order of the Attorney General without any transparency towards users.[107]

[104] Statement of the Independent Commission for Human Rights on the occasion of March 8 - International Women's Day, available via https://bit.ly/4eTrGAI

[105] Drop Site News. How Israel's Elite Intelligence Unit Targets Queer Palestinians in the West Bank. 30 August 2024. https://bit.ly/4eGaVJh

[106]- Ibid

[107]- Musawa. "Legal Memo to Dr. Hanan Ashrawi regarding the Decree-Law No. (16) of 2017 on Cybercrimes". Published in 17 September 2017 (Arabic). Check the following link: https://2cm.es/NHhl

9. Gender Dimensions: The Impact of Violations of Digital Rights on Women's Rights in Palestine

Palestinian women face compounded challenges that extend beyond traditional restrictions on movement, education, and employment. These challenges now include violations of fundamental digital rights such as freedom of expression, privacy, and access to information. Living under military occupation and within a conservative, patriarchal society, Palestinian women are caught between two forces that systematically limit their rights and deepen their marginalization.

Freedom of Expression and Access to the Internet

The right to freedom of expression is among the most affected. Women face restrictions not only in public spaces but also online, where the Internet serves as a vital platform for self-expression and information access. When internet services are shut down, women lose a crucial outlet for their voices and participation in social and political discourse, leading to further isolation.

Access to Information and Educational Opportunities

Restricted internet access deprives women of essential educational, professional, and health-related resources. This lack of access hampers their ability to make informed decisions, increases dependency on others, and weakens their autonomy. In a context where movement is often restricted—either by occupation forces or societal norms—online platforms have become critical for remote learning and employment, especially for women discouraged from traveling or interacting with men. Internet shutdowns effectively erase these limited but vital gains [108].

Gendered Impact of Conflict and Shutdowns

Armed conflict amplifies the barriers women face. Women have additional humanitarian needs, such as access to reproductive healthcare, and often bear the primary responsibility for family care. When the Internet is disrupted, these responsibilities become even harder to fulfill due to communication blackouts and disrupted access to essential services.

For men, internet shutdowns may lead to loss of income and increased psychological pressure, sometimes resulting in the displacement of frustration onto women in the form of domestic violence. In a society that tolerates male dominance, this creates an unsafe environment for women.

Digital Privacy and Social Surveillance

Internet disruptions also compromise women's digital privacy. In a patriarchal society, where women's behavior is closely monitored, the inability to communicate freely online exposes them to increased scrutiny and control by family and society. This undermines their independence and exacerbates existing gender-based oppression.

[108] Displacement of violence is a concept that refers to the transfer of violence from one person to another, or from one context to another, as a result of frustration, stress, or helplessness. Displacement occurs when an individual experiencing psychological stress or anger displaces their negative feelings onto another person, often a weaker or less threatening person. For example, if someone is under a lot of pressure at work and cannot express their anger directly towards the source of the stress, they may displace this anger onto family members.

Social Stigma and Defamation as Tools of Control

Social stigma is widely used to reinforce male dominance and suppress women's rights. Women who challenge traditional roles or participate in public activism risk being labeled as immoral or deviant, making them targets for societal backlash[109].

This stigma is weaponized by multiple actors:

- **Israeli Occupation Authorities:** Exploit personal data to discredit female activists, intimidate their families, and use shame as a form of deterrence against political expression.
- **Palestinian Authorities:** Monitor women who deviate from conservative norms or criticize political leadership. Public shaming silences dissent and fosters self-censorship.
- **Technology Companies:** Often fail to adequately protect women from online smear campaigns. Personal data and images are exploited for blackmail or public humiliation, while platforms respond slowly or ineffectively to abuse reports.

Abuse of Patriarchal Social Structures

Palestinian society's traditional, male-dominated structure is exploited by both authorities and social groups to reinforce discrimination.[110]Norms that confine women to submissive roles contribute to digital and offline violence, including:

- **“Shame laws”** that target women who speak out about taboo topics, making them susceptible to community criticism and isolation.
- **Moral stigma,** which punishes women perceived to deviate from socially accepted behavior. A single accusation of impropriety can ruin a woman’s reputation, forcing many into silence and withdrawal from public life.

[109] Consensus on this point was reached on September 16, 2024 in the (focus group) held with various Palestinian civil society institutions to explore the Palestinian digital rights scene in the period between October 7, 2023, and September 1, 2024. The meeting was attended by the Arab Center for the Development of Community Media (7amleh), Human Rights Watch, Al-Haq, the Independent Commission for Human Rights, the Jerusalem Legal Aid Center, and the Miftah.

[110]- Consensus on this point was reached on September 16, 2024 in the (focus group) held with various Palestinian civil society institutions to explore the Palestinian digital rights scene in the period between October 7, 2023, and September 1, 2024. The meeting was attended by the Arab Center for the Development of Community Media (7amleh), Human Rights Watch, Al-Haq, the Independent Commission for Human Rights, the Jerusalem Legal Aid Center, and the Miftah.

10. Conclusion

This study has illustrated the systemic and multifaceted denial of both real-world and digital rights of Palestinians, underlining the stark imbalance of power enabled by the Israeli occupation's advanced military and technological capabilities. The findings highlight how Israel exercises extensive control over the digital sphere in the occupied Palestinian territory, not as isolated incidents, but as part of a deliberate policy of domination and surveillance.

Despite existing international legal frameworks, such as the Geneva Conventions, the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), which clearly outline the obligations of an occupying power to ensure and protect human rights, these protections remain largely unenforced. The mechanisms meant to uphold international law have proven insufficient, and in many cases, completely ineffective. International accountability structures, including the United Nations and the International Court of Justice, have issued rulings and recommendations, but Israel's persistent disregard and non-compliance demonstrate a broader pattern of impunity.

This impunity is reinforced by geopolitical dynamics and a global reluctance, whether due to political alliances, strategic interests, or diplomatic caution, to hold Israel accountable through concrete legal or economic measures. As a result, Israel has been able to systematically expand its use of digital surveillance, censorship, and information manipulation, including through partnerships with major international technology firms. These partnerships not only enhance Israel's technical capabilities but also shield it from scrutiny, as global tech companies have often been complicit or passive in the face of discriminatory content moderation and surveillance practices targeting Palestinians.

Moreover, Israel benefits from a regulatory vacuum in international digital governance. There is no comprehensive, enforceable global legal framework that governs digital rights during occupation or armed conflict. This gap allows Israel to exploit legal loopholes, engage in digital repression, and control information flows without fear of legal consequence. From targeted surveillance and internet shutdowns to the suppression of Palestinian digital content, these tools are part of a wider strategy aimed at silencing dissent, controlling the narrative, and weakening Palestinian civil society.

In contrast, the Palestinian Authority (PA), despite being bound by the same human rights treaties, struggles to guarantee the digital rights of its population. This failure is not solely due to Israeli restrictions, though those play a major role, such as limited access to frequencies, infrastructure, and permits in Areas B and C, but also due to internal governance shortcomings. The PA lacks autonomy over much of the digital infrastructure, which is largely under Israeli control, severely constraining its technical and legal ability to ensure access to modern and secure telecommunications for Palestinians.

However, the study also points to a deeper issue: the PA's limited political will and institutional capacity to protect freedom of expression, digital privacy, and access to information. At times, Palestinian authorities have themselves contributed to digital repression, targeting activists and dissidents under the pretext of national security or social harmony. This dual repression, from both occupying and governing authorities, creates a digital environment marked by fear, censorship, and inequality.

Therefore, this study concludes that the Israeli occupation's use of digital tools constitutes a strategic dimension of broader control over Palestinian life. These tools are used not only to monitor and restrict but to dominate every aspect of Palestinian society, from education and economic activity to freedom of speech and political organization. The occupation's technological superiority, combined with the absence of enforceable international oversight and a fragmented Palestinian political landscape, enables a digital regime of control with few limits.

To address these realities, the international community must:

- Move beyond rhetorical condemnation to enforceable accountability mechanisms.
- Promote and support efforts to codify digital rights protections under international humanitarian and human rights law.
- Place pressure on global tech companies to apply their content moderation and privacy policies equitably and transparently.
- Encourage the development of independent digital infrastructure in Palestinian territories to reduce dependency and vulnerability.

In sum, the digital repression of Palestinians is not a side effect of occupation, it is one of its central pillars. The denial of digital rights must be recognized as both a human rights crisis and a modern form of warfare that exacerbates the already grave humanitarian and political conditions on the ground.

11. Recommendations:

The following recommendations are designed to translate the study's findings into concrete action for each key actor—Israel as the occupying power, the Palestinian National Authority, civil-society organizations, and technology companies. Drawing on international law, human-rights standards, and best practices in digital governance, they aim to restore and protect Palestinians' real and digital rights, close accountability gaps, and foster an environment in which freedom of expression, privacy, access to information, and digital inclusion can flourish.

1. Occupying Power: State of Israel

1.1 Comply with the ICJ Ruling

Israel's failure to implement the International Court of Justice's advisory opinion on the Wall reflects a wider pattern of disregard for binding and non-binding international judgments. To break this cycle, Israel must publicly acknowledge the ICJ's finding that its prolonged occupation and associated measures are unlawful. This should be followed by concrete steps, such as dismantling illegal barriers, ending settlement expansion, and allowing unfettered Palestinian movement, so that ICJ principles become lived realities rather than abstract legal statements.

1.2 Uphold International Humanitarian and Human Rights Law

The Fourth Geneva Convention and the ICCPR impose clear limits on the use of force and the treatment of civilians under occupation. Yet reports from UN bodies and NGOs chronicle repeated incidents of excessive force, arbitrary detention, and collective punishment—often facilitated by digital surveillance and communication blackouts. Israel must cease these practices, open investigations into alleged abuses, and criminally prosecute responsible individuals. Transparent, independent oversight, perhaps via a joint UN–ICRC panel, would reinforce compliance and deter future violations.

1.3 Restore Digital Rights and Infrastructure

Internet shutdowns, spectrum denial, and the obstruction of Palestinian telecom projects serve as tools of control. Israel should grant Palestinian operators full access to radio frequency spectrum and allow the construction and maintenance of local telecom towers without undue military or bureaucratic impediments. It should also refrain from severing electricity or fuel supplies that render networks inoperable. Restored connectivity would not only protect human rights but also foster economic development, telemedicine, and remote education, benefitting Israelis and Palestinians alike.

2. Palestinian National Authority (PNA)

2.1 Advance Diplomatic Advocacy

While the PA's diplomatic efforts to end the occupation have long been stymied, digital-rights abuses offer an additional lever. The PA should file formal complaints with the UN Special Rapporteur on freedom of expression, submit shadow reports to the UN Human Rights Committee, and work with friendly states to push for a Security Council resolution addressing internet shutdowns as a form of collective punishment. By framing digital-rights violations as core human-rights issues, the PA can build broader coalitions that transcend geopolitics.

2.2 Align Domestic Law with International Standards

Current Palestinian Cybercrime and anti-terrorism laws contain vaguely worded provisions that police online speech, chill journalism, and empower secretive surveillance. The PA must repeal or amend Articles 39 and 45, narrowing definitions of "incitement" and guaranteeing due process for online expression. Clear guidelines for data retention, law-enforcement access, and judicial oversight should be codified, ensuring that any limitation on digital rights is lawful, necessary, and proportionate.

2.3 Reform Governance and Judicial Independence

Effective redress for digital-rights abuses requires trust in impartial institutions. The PA should revise its judicial-appointments process to insulate judges from executive interference, establish a dedicated Digital Rights Tribunal or ombudsperson empowered to hear complaints, and guarantee that victims of online censorship or surveillance can seek compensation. Civil-society stakeholders should be included in monitoring these reforms to bolster transparency.

2.4 Strengthen Civil Society and Gender Equality

Women's rights organizations, independent media outlets, and digital-security NGOs must be recognized as essential partners. The PA can institutionalize this relationship by creating grant programs for digital-rights projects, ensuring legal protection for human-rights defenders, and launching nationwide campaigns to combat online gender-based violence. Training workshops, run in partnership with international experts, can equip activists and journalists with the tools to mitigate surveillance, encrypt communications, and document abuses safely.

3. Human-Rights Defenders and Civil-Society Organizations

3.1 Mainstream Digital Rights

Traditional monitoring frameworks often focus on physical checkpoints, home demolitions, or detention statistics. Yet digital repression, censorship, algorithmic bias, coordinated takedowns, can be equally devastating. NGOs must integrate digital metrics into their reporting, adopting tools such as network-measurement apps to detect throttling or shutdowns in real time, and cataloguing takedown notices and account suspensions issued by platforms. This holistic approach will expose the full spectrum of rights violations.

3.2 Pursue Accountability Through All Avenues

Where domestic remedies fail, strategic litigation can open new pathways. Civil-society coalitions should support cases before the International Criminal Court on war-crime charges related to deliberate communication blackouts or attacks on civilian infrastructure. They can also facilitate universal-jurisdiction suits in Europe or Latin America against arms-industry actors whose technology aids digital repression. Parallelly, complaints to UN treaty bodies, backed by robust evidence dossiers, will keep pressure on states and corporations.

3.3 Coordinate Advocacy and Capacity-Building

Fragmentation among NGOs leaves gaps in expertise and geographic reach. Civil-society networks should establish a shared digital-rights rapid response team, pooling legal counsel, technical analysts, and communications specialists. Joint trainings, on secure messaging apps, metadata hygiene, and open-source investigative techniques, will elevate the entire sector's capacity. Regular convenings can align messaging, ensure consistent data collection, and enable swift, coordinated responses to emergent digital-rights crises.

4. Technology Companies (Meta, TikTok, X, YouTube, Telegram, etc.)

4.1 Adhere to the UN Guiding Principles on Business and Human Rights

Platform operators must treat digital-rights due diligence as an ongoing responsibility. This includes commissioning independent human-rights impact assessments of content-moderation policies, algorithmic amplification, and data-sharing practices. Findings, both positive and negative, should be published in annual human-rights reports, with clear remediation plans for any identified harms.

4.2 Ensure Equitable Content Moderation

Algorithms and moderation teams often lack linguistic or contextual understanding of Palestinian discourse, leading to disproportionate takedowns. Companies should hire native speakers, invest in regional expertise, and co-create community standards with local civil-society groups. Transparent appeal mechanisms, complete with human review and clear timelines, must be guaranteed for users whose content is removed.

4.3 Protect User Privacy and Data

Platforms should minimize data collection, retaining only what is strictly necessary for service operation, and encrypt data at rest and in transit. They must refuse security or surveillance demands that lack a clear legal basis under international human-rights norms, even if presented with domestic warrants. When governments do submit valid requests, companies should publish granular transparency reports detailing request numbers, compliance rates, and legal justifications.

4.4 Refuse to Facilitate Human-Rights Abuses

Tech firms must adopt a policy of “no complicity” in state-imposed shutdowns or censorship. This means declining any technical assistance, such as routing or filtering services, that contributes to internet disruptions. Where feasible, platforms could deploy mirror sites or alternate communications channels (e.g., peer-to-peer messaging) to help users maintain connectivity during shutdowns, in alignment with the principles of life, health, and expression.

By embedding these recommendations into law, policy, corporate practice, and grassroots action, stakeholders can begin to reverse the process of digital entrapment that has deepened Palestinians’ marginalization. Collective commitment, backed by political will, technical innovation, and international solidarity, is essential to ensure that digital rights are recognized not as optional add-ons but as fundamental human rights in both peace and conflict.

12. References

European Court of Human Rights: Ahmet Yıldırım v. Turkey; European Court of Human Rights: Cengiz and Others v. Turkey

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

UN Human Rights Committee (HRC), General comment no. 34, Article 19, Freedoms of opinion and expression, CCPR/C/GC/34 , 12 September 2011, https://bit.ly/3Nry7z7

UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, 8 April 1988, https://bit.ly/4dIGRePGeneral comment no (34) on the right to freedom of expression, 2011.

Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights Report of the Office of the United Nations High Commissioner for Human Rights, https://bit.ly/404DPP2

The UN Special Rapporteur on freedom of opinion and expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on freedom of expression and the ACHPR Special Rapporteur on freedom of expression and access to information.

UN GeneralAssembly, Report of the SpecialRapporteur on the promotion and protection of the right to freedomof opinion and expression, UN Doc.A/71/373, available at: https://bit.ly/4gWqCxw

UN GeneralAssembly, Report of the Officeof the United Nations High Commissioner forHumanRights on Internetshutdowns: trends, causes,legal implications and impacts on a range of human rights, UN Doc. A/HRC/50/55, available at: https://bit.ly/3A9c4dg

UN Human Rights Council Resolution (A/HRC/RES/32/13) on the Promotion, Protection, and Enjoyment of Human Rights on the Internet.

UN GeneralAssembly, Road map for digitalcooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation, UN Doc. A/74/821, para. 41, available at: https://bit.ly/4eHbO4v

Internet Rights & Principles Coalition, The charter of human rights and principles for the internet - United Nations https://bit.ly/3U9wn17

Access Now, #KeepItOn: Telecommunications blackout in the Gaza Strip is an attack on human rights,available at: https://bit.ly/3BLEAlR13 October 2023.

Access Now - Palestine unplugged: how Israel disrupts Gaza's internet, available at: Palestine unplugged: how Israel disrupts Gaza's internet - Access Now 10 November 2023.

The New York Times, These WorkersAre Risking Their Lives to Restore Gaza's Phone Network,available at: https://www.nytimes.com/2024/03/13/world/middleeast/gaza-phone-networks.html, 13 March 2024.

Jawwal's statement on 13 January 2024: https://bit.ly/3YjToRo
+972 Magazine,A Gaza team went to repair a telecoms machine.An Israeli tank fired at them, available at: https://bit.ly/4h2VxIu, 1 May 2024

The New York Times, 34 Hours of Fear: The Blackout That Cut Gaza Off From the World, available at: https://nyti.ms/3ZXhhzz , 29 October 2023.

International Courtof Justice, Advisoryopinion of the International Courtof Justice on the Legal Consequences of the Construction of a Wallin the Occupied Palestinian Territory, available at: https://bit.ly/3A9cJLM 9 July 2004.

Adalah's report to the UN Special Rapporteur (SR) on Freedom of Opinion and Expression: Threats to Palestinians' FoE rights in Israel post-7 October 2023. Submitted 30 June 2024.

Haaretz, Netanyahu Taps Ben-Gvir to Head Team 'Fighting Terror Incitement by Palestinians' 19.Feb,2023 Netanyahu Taps Ben-Gvir to Head Team 'Fighting Terror Incitement by Palestinians' - Israel News - Haaretz.com

Letter issued by the Minister of Education directed schools to "immediately suspend any student or employee who supports the barbaric terrorist acts currently experienced in the State of Israel is available in Hebrew at: https://bit.ly/3A54XTa

972 magazine, The orchestrated persecution of Nadera Shalhoub-Kevorkian Available at: https://bit.ly/4hi3lXhApril 30, 2024

Israeli Authorities Raid Al Jazeera After Shutdown Order' Reuters (Jerusalem/Doha, 5 May 2024) Available at: https://bit.ly/3Y4uh3J

https://bit.ly/3YmphJf
Adalah, Israel's declaration of 6 Palestinian human rights groups as 'terrorist organizations' 30/12/2021, Available at https://bit.ly/3Y3qC6j

UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), ISBN No. 92-9227-227-6, UN General Assembly, 17 July 1998. Article 7 (1) (E).

Human rights watch, Gaza: Israeli Military's Digital Tools Risk Civilian Harm, Jerusalem, September 10, 2024. Available at: https://bit.ly/482F17r

The Guardian, 'The Gospel': how Israel uses AI to select bombing targets in Gaza, 1 Dec 2023. Available at: https://bit.ly/3NmcsZ0

Antonio Coco, Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes, Journal of International Criminal Justice, Volume 21, Issue 5, November 2023, Pages 1077–1096, https://doi.org/10.1093/jicj/mqad034

Human Rights Watch Report, Meta's Broken Promises, December 21, 2023. Available at: https://bit.ly/403Hcph

7amleh- The Arab Center for the Advancement of Social Media, Meta, let Palestine Speak Campaign Q&A. Available at: https://meta.7amleh.org/Q&A

UN Guiding Principles for Business and Human Rights. Namely principles 11-14.
Rome statute, articles 7, 8.
Aljazeera - What is Project Nimbus, and why are Google workers protesting Israel deal? 23, Apr, 2024. Available at: https://bit.ly/4dSQ1FS
The Times of Israel, Israel signs deal for cloud services with Google, Amazon, 24 May 2021. Available at: https://bit.ly/401Xkra
The Guardian, We are Google and Amazon workers. We condemn Project Nimbus, We cannot support our employer's decision to supply the Israeli military and government technology that is used to harm Palestinians. 12 Oct 2021 https://bit.ly/3Y31D2Y
United Nations Human rights, Office of the High Commissioner, Status of Ratification Interactive Dashboard https://bit.ly/4dQktAe, Accessed 15, Sep, 2024
Human Rights Watch Report, Meta's Broken Promises, December 21, 2023. Available at: https://bit.ly/403Hcph

Drop site news, How Israel's Elite Intelligence Unit Targets Queer Palestinians in the West Bank, Aug 30, 2024 https://bit.ly/4eGaVJh

UNGA, Res 67/168.
A/HRC/RES/32/13
E/C.12/1/Add.27.
A/HRC/28/44
A/HRC/12/37
A/HRC/8/17
A/69/348
90 E/C.12/1/Add
CCPR/C/ISR/CO
2-4/CRC/C/ISR/CO
CERD/C/IRS/CO/14-16
A/AHRC/28/44

13. Annexes:

Annex (1): Limitation of the Right to Freedom of Expression by the Israeli domestic law			
#	Criterion required by international law to limit this right	Description of criterion	Shortcomings of Israeli domestic law
1	**Legality**	There must be a clear and explicit legal framework that regulates the instances in which freedom of expression may be restricted, with reference to the instances listed in Article 19 of the International Covenant on Civil and Political Rights (ICCPR). This requires not merely stating broad terms that are susceptible to misinterpretation, as follows: 1. For the protection of national security and public order, it is not permissible to use the terms: 'spreading sectarian strife', 'causing harm to the public interest', 'incitement to violence', 'spreading sedition', or 'outraging public decency' without providing clear definitions of these concepts and terms. 2. To respect the rights and reputations of others, it is not permissible to use the terms 'high ranks', 'degrading', 'defamation', 'slander', and 'vilification' without providing clear definitions of these concepts and terms[111].	**A. Counterterrorism Act of 2016** Article 24 uses broad terms that allow leeway for limitations to be imposed on freedom of expression that would be illegal under international law. For example, the Act states that "publishing words of praise, support or sympathy, waving a flag, displaying or publishing a symbol, displaying or operating" are acts that constitute a crime punishable by imprisonment. **B. Penal Code of 1977** Article 173 prohibits the use of any expression that offends "religious beliefs" or the feelings of others, but does not define this more explicitly, leaving it open to be applied broadly by the authorities to limit freedom of expression, with the result that legitimate forms of freedom of expression may be prosecuted under the laws prohibiting defamation, libel, and slander. **C. Freedom of Information Act of 1998** Article 9 lists instances in which the state and its agencies are required to withhold information from the public: (1) "Information the disclosure of which could compromise the security of the state, its foreign relations, public security, or the security or well-being of a person. (2) Information concerning issues.

[111] General comment no (34) on the right to freedom of expression, 2011. Available at:

2	**Necessity**	The reason for the limitation of freedom of expression must be urgent, essential to the preservation of public and compelling legitimate interests, and meet one of the criteria listed in Article 19, paragraph 3: “respect of the rights or reputations of others” or “protection of national security or of public order or of public health or morals”. The UN Human Rights Committee has noted that the scope of this freedom cannot be assessed using “margin or discretion.” To enable the Committee to perform this task, the State party must demonstrate the precise nature of the threat, with reference to the conditions stated in Article 19(3), that deemed it necessary to restrict freedom of expression[112].	**A. The Counterterrorism Law of 2016** On the contrary, the publication of any word or any news that is considered sympathy or support for an organization that Israel considers terrorist is itself a crime, even if it does not cause any harm or danger and without any necessity to punish the person. **B. Penal Code of 1977** This law does not contain specific criterion for determining what constitutes offending another person's religious beliefs. The religious context in which this law is applied in occupied Jerusalem is extraordinarily complex due to the multiplicity of religions in the city. The ambiguity of the law, applied illegally by an occupying state to a complex political and religious environment in an occupied territory, results in a reality in which virtually anything an Arab, whether Muslim or Christian, does against a Jew may be considered a violation of their freedom and religious beliefs and lead to their punishment At the same time, despite direct violations by Jews against Muslims and Christians and their holy sites, there is great difficulty in proving that there is a violation of their religious freedom and very few cases where a Jew is punished for these crimes.

[112] General comment no (34) on the right to freedom of expression, 2011. Paragraph 36.

			C. Freedom of Information Act of 1998 **b.** This law states that information may be withheld from the public on the grounds of preservation of state security, public order or the welfare of a person; however, as Israel has been in a continuous state of emergency since its creation in 1948, this can be used as a pretext to withhold information broadly. As everything that is Arab threatens security and order, this article strongly opposes international law As this law lacks criterion for what constitutes a threat to security and order, it can be widely applied to limit freedom of expression on the basis of whatever the Israeli Minister of Defense deems a threat to public security or state order in the context of an occupied city.
3	**Proportionality**	**-** A clear link must be established between the limitation and the interest for which it was imposed. **-** The limitation must be within the limits of what is useful and essential in order to preserve this interest.	**The Nakba Law of 2011. This law considers the fact that an organization considers the 1948 Nakba to be a day of mourning for the victims of war a sufficient reason to withhold funding and support, even if it is a non-profit and humanitarian organization.** **This provision is fundamentally contrary to the principle of proportionality and leads to an unjustified restriction of the right of freedom of expression.** **The 2016 Terrorism Law. In a clear contradiction of the principle of proportionality, this law states that publishing any word expressing sympathy or support for any organization or group that Israel considers terrorist is punishable by up to five years in prison.** **The Entry into Israel Law of 1952. Article 2 of the law states that an organization or person who calls for a boycott of Israel as part of their right to freedom of expression will be denied a visa to enter Israel.**

4	**Judicial order from a neutral judicial authority**		None of the Israeli legislation discussed above requires judicial authorization; rather, the law is interpreted and enforced at the discretion of executive government authorities. It is clear that anyone who has an objection to these policies can apply to the court to have them annulled, and only then will the judiciary consider the matter.
Right to Privacy			
	Criterion required by international law to limit this right	**Description of criterion**	**Shortcomings of Israeli domestic law**
	Legality	The concept of legality means that any interference with the right to privacy must have a basis in law. The law must conform to the principles and provisions of the International Covenant on Civil and Political Rights (ICCPR). Thus, interference that does not have a legal basis or is based on domestic law that fundamentally violates Article 17 of the International Covenant on Civil and Political Rights is unlawful and constitutes a violation of the right to privacy. In terms of the concept of arbitrariness: The Human Rights Committee's Comment No. 16 makes two points regarding the prohibition of arbitrary interference: - Interference that is based on domestic law that is fundamentally contrary to the Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and its principles and purposes is prohibited.	**A. The Protection of Privacy Law of 1981** **This law contains clear definitions that show that everyone has the right to respect of their privacy. It also details the forms of infringement of this privacy and considers it a criminal act and a civil offense requiring compensation. It also** prohibits the direct or indirect use of the personal data of citizens receiving services from companies and institutions with which they share this information without their prior written consent, under penalty of legal liability. **Some of the articles define a margin for infringement of privacy without accountability. For example, Article 18 states that a publisher will not be penalized for infringing on the privacy of others if he has a professional ethical or legal duty to publish (no other criteria are specified as to what constitutes such a duty). In another paragraph, publication for the purpose of defending the publisher's personal interest is permitted without limits or restrictions for this or other circumstances that are broadly defined for which infringement of privacy is permitted.**

		- Interference must be appropriate to the specific circumstances in which it is legally permissible. In addition, the law governing this right must meet the following criteria: - The language of the law must be accessible to the average person (published in the official manner). - The law must link the concept of interference with the right to privacy to specific objectives with clear definitions. - The law must provide safeguards against arbitrary interference (e.g., disciplinary penalties for anyone who exceeds their powers). - The law must detail the procedures to be followed for such interference, indicate who has the authority to intervene, and define the conditions under which such interference may take place.	**Article 19 completely exempts security authorities from any accountability in the event of "reasonable" interference with privacy for the purpose of performing their work. However, these authorities are not named and no standard for "reasonable" is defined.**
	Necessity and proportionality	Necessity refers to the condition that any interference with the right to privacy must be essential to the attainment of a particular, and urgent, goal. Proportionality means: - There must be a logical link between the interference and the specific aim for which it was legislated and the interference must be carried out within the limits of that objective. - The interference must be within the limits of what is useful and essential for the achievement of the specified objective.	Criminal Procedure (Arrest and Search) Order 1969 Section 25(b) applicable from 15.05.2023 to 30.06.2025 states: "A police officer may, without a search warrant, enter and search any house or place if: (3) a reasonable suspicion arises that there is a weapon or a substantial part of a weapon in the house or place that could be used as evidence of an offense under section 144 (possession of a weapon without a license) of the Penal Code, if no action is taken. Failure to search immediately would frustrate the purpose of the search, and a search warrant cannot be obtained because the search must be conducted immediately to prevent the disappearance or damage to the evidence. (2) Reasonable suspicion has arisen that there is documentation or a camera in the home or premises that may be

		- There must be a specific and particular situation in which there is a reasonable doubt that there is a need to interfere with the right to privacy. The legality, necessity, and relativity of the interference must be determined separately for each specific case That is, the nature of the interference may differ according to the case but the basic principles governing that interference must be met. What is considered legal, necessary and proportionate in a specific case may be prohibited in another case.	evidence of the commission of a serious crime or offense under sections 144a, b or 340a(b) of the Penal Code, if failure to conduct a search immediately would frustrate the purpose of the search, and it is not possible to obtain a search warrant due to the necessity to conduct a search immediately to prevent the loss of or damage to the evidentiary objects. The Prevention of Eavesdropping Act of 1977, Article 4, states: "The Minister may, if so requested in writing by the head of the security authority, and if, after considering the extent of the invasion of privacy, he is satisfied that it is necessary for reasons of national security, authorize in writing the interception of telephone conversations." This language is broad, failing to provide criteria for a determination of a national security concern. The intervention is disproportionate.
	Judicial permission (order)	This principle establishes the rule that any interference with the right to privacy requires judicial authorization in order to limit the abuse of executive powers. The judicial authority must be impartial and independent, meaning that it is able to carry out its work without any external influence from the executive or legislative branches or any other entity. The judicial authorization must specify the persons whose information or communications are to be accessed, the purpose of the interference, the information that is expected to be obtained with the greatest specificity, the persons who are permitted access to the information, and the time frame in which the interference takes place.	The Criminal Procedure (Arrest and Search) Order of 1969. Article 23 of the law clarifies that searches in private homes and properties for the purposes of investigating a crime shall be ordered by the competent court. Article 23a clarifies that the search of computers and other smart devices is also considered a search and must be carried out by computer specialists and only on the basis of a court order that clearly spells out what is to be searched (i.e. not everything can be searched) so as not to violate privacy. The 1979 Wiretap Act does not apply to this type of search. Article 25a identifies some exceptional instances in which the police are permitted to search without a court order, such as believing that a crime is taking place on the premises, requesting help from someone inside the premises, or in the case of pursuing a fugitive. However, in all of the above-mentioned legal and proportionality clauses, the need to obtain a court order is not stipulated.

Annex (2): Limitation of the Right to Freedom of Expression By PA			
#	Criterion required by international law to limit this right	Description of criterion	The contradiction between local law and international law
5	**Legality**	There must be a clear and explicit legal framework that regulates the instances in which freedom of expression may be restricted, with reference to the instances listed in Article 19 of the International Covenant on Civil and Political Rights (ICCPR). This requires not merely stating broad terms that are susceptible to misinterpretation, as follows: 1. For the protection of national security and public order, it is not permissible to use the terms: 'spreading sectarian strife', 'causing harm to the public interest', 'incitement to violence', 'spreading sedition', or 'outraging public decency' without providing clear definitions of these concepts and terms. 2. To respect the rights and reputations of others, it is not permissible to use the terms 'high ranks', 'degrading', 'defamation', 'slander', and 'vilification' without providing clear definitions of these concepts and terms.	**b. Cybercrime Law No. (10) of 2018** - Article 39 uses several broad terms that provide leeway for restrictions to be imposed that would be illegal under international law. The article states: "The competent authorities of investigation and seizure, in the event they monitor hosted electronic websites, which broadcast either inside or outside the State, posting any expressions, figures, images, films, propaganda materials or others which may threaten national security, public order or public morals, shall be entitled to submit a report thereon to the Attorney General or one of his assistants and request permission to block the broadcast of the electronic website(s) or block some of their links." - Article 31 states: "In accordance with the prescribed legal procedures, the service provider shall adhere to the following [...] 2. Block the link or content or application on the electronic network, based on the orders issued forth thereto from the judicial authorities without prejudice to the procedures provided for under Article 39 of this Law by Decree." - Article 45: "Each person who perpetrates an act that constitutes a crime under any effective piece of legislation, and not provided for under this Law by Decree, using the electronic network or a means of information technology, or is involved as an accomplice, abettor or accessory to its perpetration, shall be liable to the same penalty which is prescribed for such crime under that piece of legislation."

		- There must be a specific and particular situation in which there is a reasonable doubt that there is a need to interfere with the right to privacy. The legality, necessity, and relativity of the interference must be determined separately for each specific case That is, the nature of the interference may differ according to the case but the basic principles governing that interference must be met. What is considered legal, necessary and proportionate in a specific case may be prohibited in another case.	- Several Articles (188-199) could be misappropriated by the authorities to limit freedom of expression or to interpret certain forms of freedom as criminal behavior such as defamation, libel, or slander. **c. Printing and Publishing Law No. 9 of 1995** - Article 7 uses broad and undefined terms; this could be exploited to limit freedom of expression. The Article states: "Publications must refrain from publishing anything that contradicts the principles of freedom, national responsibility, human rights, and respect for the truth, and consider freedom of thought, opinion, expression, and information as a right for citizens as well as for themselves. Periodical publications directed at children and adolescents must not include any pictures, stories, or news that violate Palestinian morals, values and traditions." - Article 37 of the law contains broad and undefined terms that could be used as a legal basis for restricting freedom of expression. The Article states: "A- It is prohibited for a publication to publish the following: 1- Any confidential information about the police and public security forces, their weapons, equipment, locations, movements, or training. 2- Articles and materials that include denigrating religions and sects whose freedom is legally guaranteed. 3- Articles that are likely to harm national unity, incite the commission of crimes, sow hatred, discord, disharmony and incite sectarianism among members of society. 4- Proceedings of the secret sessions of the National Council and the Council of Ministers of the Authority. 5- Articles or news intended to undermine confidence in the national currency. 6- Articles or news that may offend the dignity or personal freedoms of individuals or damage their reputation. 7- News, reports, letters, articles, and pictures that are contrary to public morals and ethics."

		- There must be a specific and particular situation in which there is a reasonable doubt that there is a need to interfere with the right to privacy. The legality, necessity, and relativity of the interference must be determined separately for each specific case That is, the nature of the interference may differ according to the case but the basic principles governing that interference must be met. What is considered legal, necessary and proportionate in a specific case may be prohibited in another case.	**D. Penal Code No. 16 of 1960** It is worth noting that Article 45 of the Cybercrime Law stipulates that anyone who commits an act that constitutes a crime under any legislation using the Internet or information technology, or participates in or incites another person to commit such a crime, that is not stipulated in a decision of the Cybercrime Law, shall be liable for the same penalty prescribed for that crime in that legislation. This refers to the Penal Code, which contains several broad terms that allow license to limit freedom of expression, such as Article 131 of the Code, which punishes anyone who knowingly spreads false or exaggerated reports abroad that might weaken the state's standing or prestige. In this case, a person will be liable for the same penalty stipulated in the previous article. If the person broadcasts such news believing it to be true, he shall be punished by imprisonment for a period of not less than three months. Article 130 stipulates a penalty of temporary hard labor for any person who, in time of war or when the outbreak of war is anticipated, disseminates propaganda aimed at weakening patriotic sentiment or stirring up racial or sectarian strife.
6	**Necessity**	The restriction is essential and urgent to preserve public and compelling legitimate interests and falls under what is mentioned in Article 19(3) of the ICCPR. The UN Human Rights Committee has noted that the scope of this freedom cannot be assessed using "margin or discretion." In order to enable the Committee to perform its task, the State party in the case at hand must ensure that the restriction is necessary and urgent for the preservation of legitimate, public, and compelling interests and falls under Article 19(3). To enable the Committee to perform this task, the State party in the specific case must	**b. Cybercrime Law No. (10) of 2018** When the competent authorities monitor websites that contain content that threatens national security, public order, or public morality, they must submit a report to the Public Prosecutor's office to request permission to block a website or specific pages of the site. The Public Prosecutor must submit the blocking request to the Magistrate's Court within 24 hours, accompanied by an explanatory memorandum. The court must issue its decision on the same day and set a suspension period for a maximum of six months, renewable in accordance with the applicable legal procedures.

		demonstrate the precise nature of the threat to any of the grounds listed in Article 19(3) that led it to impose the necessary restrictions on freedom of expression[113].	In this context, it is at the discretion of the Prosecutor's Office and the court to determine what falls under "public order" and the extent to which it is necessary to intervene to limit freedom of expression to protect public order. Article 39 of the Cybercrime Law, which authorizes the blocking of websites based on reports from investigative and seizure authorities (security agencies) that are submitted to the office of the Public Prosecutor to obtain permission from the Magistrate's Court to block them within 24 hours, under broad terms related to national security, public order, and public morality.
7	**Proportionality**	**-** There is a logical link between the restriction and the interest for which it was imposed. **-** The restriction must be within the limits of what is useful and essential in order to preserve this interest.	**Printing and Publishing Law No. 9 of 1995** The public right of action for the periodical publication offenses stipulated in this Law shall be brought against the responsible editor-in-chief and the author of the article as original perpetrators. The owner of the press publication shall be jointly liable with them for the personal rights resulting from such offenses and the expenses of the trial, without incurring any criminal liability unless his actual participation or involvement in the offense is proven. The public right lawsuit for the offenses of non-periodical publications stipulated in this law shall be brought against its author as the original perpetrator and its publisher as an accomplice. If the author or publisher of the publication is unknown, the owner of the printing press will be prosecuted. The punitive measures contained in this article that lead to the personal prosecution of journalists as a result of their publications are fundamentally contrary to the principle of proportionality and lead to an unjustified restriction of publishing rights[114].

[113] General comment no 34 on the right to freedom of expression, 2011. Paragraph 36.

[114] Law No. (9) of 1995 regarding printing and publishing, Article 42.

			Article (37) states: Prohibited Publications A- It is prohibited for a publication to publish the following: 1- Any confidential information about the police and public security forces, their weapons, equipment, locations, movements or training. 2- Articles and materials that include insulting religions and sects whose freedom is guaranteed by law. 3- Articles that are likely to harm national unity, incite the commission of crimes, sow hatred, discord, disharmony and incite sectarianism among members of society. 4- Proceedings of the secret sessions of the National Council and the Council of Ministers of the Authority 5- Articles or news intended to undermine confidence in the national currency. 6- Articles or news that may offend the dignity or personal freedoms of individuals or damage their reputation. 7- News, reports, letters, articles and pictures that are contrary to public morals and ethics. 8- Advertisements that promote medicines, medical preparations, cigarettes and the like, unless their publication is previously authorized by the Ministry of Health. B- It is forbidden to import publications from abroad if they contain what is prohibited to be published according to the provisions of this law.
8	**Judicial permission from a neutral judicial authority**		Many of the laws regulating the right to freedom of expression impose restrictions with “judicial authorization.” While it might be presumed that such authorization would be made in alignment with international standards, this is not the case. In Palestine, judicial appointments are made by the President of the Palestinian National Authority based on the recommendation of the Supreme Judicial Council through initial appointment, promotion based on seniority taking into account

			competence, appointment from staff from the office of the Public Prosecutor, or borrowing from brotherly countries. This may affect the decisions of judges by potentially interfering with the executive authority and limiting their independence.
Limitations to the Right to Privacy			
	Criterion required by international law to limit this right	**Description of criterion**	**Shortcomings of Palestinian domestic law**
	Legality	The concept of legality requires that any limitation imposed on the right to privacy must have a basis in law. Such law must conform to the principles and provisions of the International Covenant on Civil and Political Rights (ICCPR). Thus, interference with the right to privacy that does not have a legal basis, or is based on domestic law that fundamentally violates Article 17 of the ICCPR is unlawful and constitutes a violation of the right to privacy. With regard to the concept of arbitrariness, Comment No. 16 by the Human Rights Committee on the prohibition of arbitrary interference makes two points: - It emphasizes that interference based on law that fundamentally contradicts Article 17 and the principles and purposes of the ICCPRis prohibited. - It mandates that any interference with the right to privacy must be appropriate to the specific circumstances in which it is legally permissible and that the law governing this right must satisfy the following conditions: - Be easily accessible to the average person (published in the official manner).	**B. Palestinian Basic Law** The Palestinian Basic Law enshrines several basic rights that have bearing on privacy. Article 32 provides protection against attacks on personal freedoms and privacy, and guarantees fair compensation to those affected. Articles 110 and 111 specify the conditions and limitations of a state of emergency, indicating that rights and freedoms may be restricted only to the extent necessary to achieve the declared objective. While the phrasing of the article aligns with international standards, the article does not contain effective safeguards against the arbitrary use of power or mandate accountability mechanisms explicitly; nor does it reference other laws that provide for this. **C. Cybercrime Law No. 10 of 2018** Article 31 Paragraph 1 of the law stipulates the obligation of the service provider to provide the competent authorities with subscriber information that helps “uncover the truth” at the request of the Public Prosecution or the competent court. Paragraph 3 requires service providers to retain this information for 3 years.

		- Link the concept of interference with the right to privacy to specific objectives with clear definitions. - Provide safeguards against arbitrary interference (e.g., disciplinary penalties for those who abuse their powers). - Clearly articulate the procedures required, who is authorized to intervene, and the circumstances under which the interference is permitted to take place.	It should be noted that the term "uncovering the truth" is a broad term could be misappropriated to violate the right to privacy, especially since the text of the article does not restrict this with judicial authorization. **D. Council of Ministers Decision No. 3 of 2019 on Citizens' Personal Data** This decision does not address the right to privacy specifically, but it prohibits the use of the personal data of individuals receiving services from companies and service providers, collected through direct or indirect means, for commercial purposes, without obtaining their prior permission, under the penalty of legal liability. As mechanisms for enforcing legal liability are not specified, however, this framework fails to provide protection in the event that personal data is used illegally.
8	**Necessity and proportionality**	Necessity refers to the condition that any interference with the right to privacy must be essential to achieving an urgent need to achieve a legitimate goal. Proportionality means that: - There must be a logical link between the interference and the specific goal for which it was legislated and the interference must be carried out within the limits of that goal. - The interference must be within the limits of what is useful and essential in order to achieve the specific goal.	**b. Cybercrime Law No. 10 of 2018** Article 31.1 of the Decree Law stipulates that service providers shall be obligated to provide the competent authorities with subscribers' information that helps to "uncover the truth" at the request of the Public Prosecutor or the competent court. Paragraph 3 of the Article stipulates that service providers are obligated to retain information for a period of 3 years. This article does not impose conditions of necessity and proportionality in its obligations for service providers. - Article 33 stipulates: The Public Prosecutor may obtain devices, tools, means, data, electronic information, traffic data, data related to communications traffic or its users, or subscriber information related to electronic crime.

		- There must be a specific case for which reasonable doubt can be formed about the existence of a reason for interference with the right to privacy. The legality, necessity, and relativity of the interference must be determined separately in each specific case separately. That is, the nature of the interference may differing according to the case but the basic principles governing that interference must be met. What is considered legal, necessary and proportionate in a specific case may be prohibited in another case.	Again, the criteria of necessity and proportionality are not imposed in this article. **c. Law of Penal Procedures No. 3 of 2001** The law protects the right to privacy of suspects in criminal cases. Article 51 gives special powers to the office of the Public Prosecutor to review and seize letters, messages, newspapers, publications, parcels, and telegrams related to the crime and the person who committed it at telegraph and post offices. It grants the Public Prosecutor the power to monitor wired and wireless conversations and to make recordings of conversations in a private place if a permit is obtained from a justice of the peace and on the condition that such action aid the uncovering of truth in a felony or misdemeanor punishable by imprisonment for a period of not less than one year. In addition to protecting privacy, Paragraph 3 of the Article stipulates that the seizure order or permit to monitor or record must be on reasonable grounds, and may not exceed fifteen days, except for one extension. This law applies standards of proportionality and necessity to protect the digital rights to privacy of criminal suspects.
	Judicial permission	This principle establishes the rule that any interference with the right to privacy requires judicial authorization in order to limit the abuse of executive powers. The judiciary must be neutral and independent, i.e. able to carry out its work without any external influence from the executive, legislative, or any other authority.	**Cybercrime Law No. 10 of 2018** Article 31 Paragraph 1 of the law stipulates that the service provider is obligated to provide the competent authorities with subscriber information that aids in uncovering the truth at the request of the Public Prosecutor or the competent court; this means that the Public Prosecutor can restrict the right to privacy without judicial authorization from an independent judicial authority without reference to the competent court.

		The judicial authorization must specify the persons whose information or communications will be accessed, the purpose of the interference, the information that is expected to be obtained in the greatest possible detail, the purpose for which the interference is being carried out, the persons permitted to access the information, and the time frame within which the interference will be carried out.	Article 32 gives the Public Prosecutor the authority to search for persons, places, and information technology when investigating a specific crime. The law ties this authority to the fact that the search order must be reasonable and specific. The order may be renewed more than once, as long as the justification for the measure remains. The Article also gives the Public Prosecutor the authority to authorize the direct access of law enforcement officers or their experts to search for any form of information technology to obtain data or information, provided that the law enforcement officer is qualified to deal with the special nature of cybercrime. However, the Article does not require judicial authorization from an independent judicial authority, which contradicts the essence of international principles of restricting the right to privacy. Article 34 stipulates that the office of the Public Prosecutor may order the immediate collection and provision of any data, including communications traffic, electronic information, traffic data, or subscriber information that is deemed necessary in the interest of investigations without limiting it with judicial authorization.