



Palestinian Digital Rights, Genocide, and Big Tech Accountability



7amleh - The Arab Center for the Advancement of Social Media
September 2024

Palestinian Digital Rights, Genocide, and Big Tech Accountability

Produced by: 7amleh's Advocacy Department

Designed by: Majd Shurbaji

Special Acknowledgements:

We extend our gratitude to Al Mezan Center for Human Rights for their significant contributions to the section titled "Internet and Telecommunication Blackouts as an Unlawful Method of Warfare."

This version is licensed under the following International License: Attribution-NonCommercial-NoDerivs 4.0 International
To view a copy of the license, please visit the [link](#)

Contact us:

Email: info@7amleh.org

Website: www.7amleh.org

Telephone: +972 (0) 7740 20670

Find us on social media: **7amleh**



Table of Contents

| | |
|--|-----------|
| Introduction | 4 |
| What are Digital Rights? | 7 |
| The Role of Online Platforms | 9 |
| Censorship | 9 |
| Harmful Content on Online Platforms | 12 |
| Hate Speech and Incitement to Genocide | 12 |
| Problematic Advertisements | 15 |
| Disinformation and Influence Campaigns | 16 |
| Artificial Intelligence, Data, and Automation in War | 19 |
| Artificial Intelligence in War | 20 |
| Surveillance and Facial Recognition Technologies in Gaza | 21 |
| The Automation of Killing | 22 |
| The Role of Big Tech | 23 |
| Google and Amazon’s Project Nimbus | 24 |
| Metadata and Safeguarding Right to Privacy | 26 |
| Internet and Telecommunication Blackouts as an Unlawful Method of Warfare | 27 |
| Telecommunications blackouts Amidst the Ongoing War on Gaza | 27 |
| Historical Context and Humanitarian Impact of Telecommunications Blackouts | 29 |
| Obstacles to Human Rights Documentation and Accountability | 30 |
| Violation of International Humanitarian Law | 31 |
| Recommendations | 33 |
| Big Tech, Online Platforms, & Telecommunications Companies | 33 |
| Commit to: | 34 |
| Ensure: | 34 |
| Guarantee: | 34 |
| Provide full transparency on: | 35 |
| International duty-bearers | 35 |

Introduction

We are living in unprecedented times. On January 26, 2024, the International Court of Justice (ICJ) ordered provisional measures based on the plausibility of genocide taking place in Gaza¹. This assertion was reaffirmed on May 26, 2024, when the ICJ ordered Israel to halt its military operation in Rafah, citing violations of the Genocide Convention². This brief seeks to explore the intersection of digital rights and genocide, an intersection that has been largely overlooked but is critical for understanding the full scope of the crisis. The urgency of this brief is underscored by statements from numerous UN experts and bodies. Francesca Albanese, the UN Special Rapporteur on the situation of human rights in the Occupied Palestinian Territories, has explicitly stated through her report *Anatomy of a Genocide* that "there are reasonable grounds to believe that Israel is committing genocide against Palestinians in Gaza."³ The UN Independent International Commission of Inquiry has found that Israeli authorities are responsible for "war crimes and crimes against humanity," including extermination and forcible transfer⁴. Additionally, Tlaleng Mofokeng, the UN Rapporteur on the right to health, has highlighted the severe impact of the ongoing aggression on Gazans' lives, stating: "When you have a group of people who have literally been exterminated, what else is there to declare it a genocide."⁵

Throughout the continuing war on Gaza, we came to observe how various new technologies were employed by the Israeli army, including "efficient" targeting systems⁶, semi-autonomous drones⁷, and expansive facial-recognition systems⁸, consequently furthering the suffering of the Palestinian people in Gaza. AI technologies in particular have played a troubling role in this. Israel's purported use of AI in warfare, such as the Lavender and Gospel targeting systems, has automated mass killings in Gaza and led to condemnations by several UN experts⁹. Similarly, we came to observe how various big tech companies played a role in exacerbating digital rights violations at a time when egregious violations of international humanitarian law and fundamental human rights were already taking place.

1. Order Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), International Court of Justice, 26 January, 2024, available at: www.icj-cij.org

2. Order Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), International Court of Justice, 24 May 2024, available at: www.icj-cij.org

3. "Anatomy of a Genocide - Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967", Human Rights Council, 25 March, 2024, available at: www.ohchr.org

4. Commission of Inquiry on the Occupied Palestinian Territory Concludes that Israeli Authorities and Hamas Are Both Responsible for War Crimes, Human Rights Council, June 19, 2024, available at: www.ohchr.org

5. UN rapporteur: 'No other term but genocide can be used to express Gaza situation', Middle East Monitor, 29 June, 2024, available at: www.middleeastmonitor.com

6. Brumfiel, G., Israel is using an AI system to find targets in Gaza. Experts say it's just the start, NPR, December 13 2024, available at: www.npr.org

7. Gaza: Israel systematically uses quadcopters to kill Palestinians from a close distance, EuroMed Monitor, 19 February 2024, available at: reliefweb.int

8. Frenkel, S., Israel Deploys Expansive Facial Recognition Program in Gaza, New York Times, March 27, 2024, available at: www.nytimes.com

9. OHCHR: Gaza: UN experts deplore use of purported AI to commit 'domicide' in Gaza, call for reparative approach to rebuilding, 15 April 2024, available at: www.ohchr.org

Amidst the severe violence in Gaza, the right to access information, a central component of the right to freedom of expression as enshrined in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, was severely compromised. Censorship efforts prevented Palestinians from sharing critical information with the outside world, while disinformation and coordinated influence campaigns¹⁰ by the Israeli government significantly disrupted the flow of truthful information, exacerbating the humanitarian crisis, such as by influencing the defunding of UNRWA¹¹. Additionally, telecommunications blackouts hindered the ability of individuals to access and disseminate vital information, further isolating them during the violence¹². In July, the Foreign Press Association expressed its "shock and profound disappointment" that nine months into the devastating war, Israel continues to bar independent access for the international media from Gaza, enforcing an unprecedented information blackout and raising questions about what Israel doesn't want international journalists to see¹³. The information blackout is compounded by many digital rights violations that affect Palestinians during those most difficult times when unimpeded access to information is vital for life.

The relevance of digital rights in this context cannot be overstated. This brief covers key areas such as the perceived complicity of big tech and the role of new technologies in digital rights violations amidst plausible genocide. It will cover the impact of deliberate telecommunications blackouts, the use of AI in Gaza, and the role of big tech in providing cloud computing services to parties responsible for enabling large-scale human rights violations in Gaza.

Violations of freedom of expression, censoring and silencing Palestinians, preventing them from accessing information, and sharing videos and narratives to document and broadcast the realities on the ground and other digital rights amidst plausible genocide constitute grave violations that must be addressed and confronted. Similarly, when online platforms allow hate speech and incitement on their platforms, they could be guilty of helping spread content that dehumanizes Palestinians and justifies their collective punishment, which is an illegal act in and of itself. Online platforms like Facebook, X, and YouTube have all had instances where they allowed content that dehumanizes Palestinians and justifies their collective punishment in the context of what is happening in Gaza.

10. Benjakob, O., *Israel Secretly Targeted American Lawmakers With Gaza War Influence Campaign*, Haaretz, June 5, 2024, available at: www.haaretz.com

11. Benjakob, O., *Israeli influence operation targets U.S. lawmakers on Hamas-UNRWA*, Haaretz, March 19, 2024, Available at: www.haaretz.com

12. Palestine unplugged: how Israel disrupts Gaza's internet, 10 November 2023, available at: www.accessnow.org

13. Statement by the Foreign Press Association regarding non access for foreign press to Gaza, July 7, 2024 foreignpressassociation.online

The question of complicity by companies like Meta, Google, and Amazon, whether their role constitutes of inadvertently feeding data to Israeli AI-targeting systems or cooperating with the Israeli Ministry of Defense and the Israeli army, will help us assess those companies' commitment to safeguarding human rights, their commitment to protecting at-risk people amidst genocide, and explore strategies to achieve big tech accountability.

This brief seeks to highlight the critical role that digital rights play in the context of genocide. It aims to equip readers with a clear understanding of how technology is being used to perpetrate and exacerbate human rights violations, and to emphasize the need for urgent action to protect digital rights, develop accountability mechanisms, and avert Genocide.

What are Digital Rights?

Digital human rights are fundamental rights and freedoms inherent to all human beings, both online and offline. Those rights are interrelated, interdependent, and indivisible, requiring protection from discrimination and arbitrary interference. State actors and private actors have obligations under international law to respect, protect, and fulfill these rights. Just as human rights are supposed to be protected offline, they must also be safeguarded online.

The right to access the internet is increasingly recognized as a fundamental human right, essential for participating in the modern world. It enables individuals to share and acquire knowledge, engage in social networking, organize politically, and participate in the economy. This right includes access to both the physical infrastructure required for internet connectivity and the online content itself. It must be protected from deliberate manipulation and discrimination based on race, color, sex, language, religion, political opinion, national or social origin and ethnicity. Responsible authorities must ensure that internet access is widely available and accessible, particularly during times of crisis as witnessed in Gaza.

The rights to freedom of expression, opinion, and information are crucial for the free flow of ideas and information online. These rights, protected under Article 19 of the International Covenant on Civil and Political Rights (ICCPR)¹⁴, include the ability to seek, receive, and impart information and ideas without interference, regardless of borders. Safeguards must be in place to allow individuals to express themselves online, facilitating the free flow of information and ideas.

The rights to peaceful assembly, freedom of association, and participation extend to online spaces. Articles 21 and 22 of the ICCPR guarantee these rights, allowing individuals to practice freedom of assembly and association online.

The right to privacy, including data protection, is protected under Article 17 of the ICCPR. It protects individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence through messaging services such as Meta's WhatsApp. Privacy must be safeguarded against mass surveillance, interception of digital communications, and unauthorized data collection. Violations of privacy can impact other rights, including the rights to life, liberty, security, freedom from torture, health, due process, freedom of movement, assembly, association, and expression.

14. International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI), adopted 16 December 1966, available here: www.ohchr.org

The right to liberty and security of person, as articulated in Article 9 of the ICCPR, asserts that "no one shall be subjected to arbitrary arrest or detention" and that deprivation of liberty must be lawful. Online, this right includes protection against cybercrimes and ensuring secure Internet connections.

The right to non-discrimination, alongside equality before the law, is fundamental to international human rights law, as emphasized in the ICCPR and the Universal Declaration of Human Rights (UDHR)¹⁵. Online, this right ensures equal access to the Internet and protection from discriminatory practices based on various statuses.

Non-state actors, including big tech companies, have obligations under international frameworks like the UN Guiding Principles on Business and Human Rights¹⁶ to respect, protect, and remedy digital and human rights. These principles mandate that businesses must conduct due diligence to identify, prevent, mitigate, and account for how they address their impacts on human rights. They must also provide for or cooperate in remediation processes for any adverse human rights impacts they cause or contribute to.

In the context of genocide and the war on Gaza, the protection of digital rights is paramount. Tech companies and online platforms play a critical role in documenting human rights abuses, sharing information, and mobilizing support. Systematic censorship and discriminatory content moderation policies by these platforms, as seen in the suppression of Palestinian voices, undermine these digital rights. The right to access the Internet, freedom of expression, and privacy are all essential for individuals to share their experiences, seek justice, and advocate for their rights. Violations of these rights during such critical times not only silence marginalized voices but also hinder efforts to address and prevent atrocities. Thus, the intersection of digital rights and genocide in Gaza highlights the urgent need for robust protections and accountability to ensure that digital spaces remain open and equitable for all.

15. Universal Declaration of Human Rights, General Assembly resolution 217 A, adopted 10 December 1948, available here: www.un.org

16. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, UN - OHCHR, 2011, Available at: www.ohchr.org

The Role of Online Platforms

Censorship

The discriminatory content moderation policies of social media companies have led to unprecedented and systematic censorship of Palestinian voices and content related to Palestine throughout the ongoing war on Gaza. Particularly of concern were Palestinian journalists and content creators in Gaza who faced restrictions and disproportionate censorship on their social media profiles across online platforms. Violation of the rights to freedom of expression, opinion and information amidst ongoing aggression raised serious concern about the role of tech companies exacerbating fundamental rights violations amidst genocide.

From October 7th 2023, to July 1st 2024, the Palestinian Observatory of Digital Rights Violations (7or) documented more than 1,350 instances of online censorship across major platforms¹⁷. Those violations varied between suspensions, content takedowns, account restrictions, reduced distribution, and others. The biggest offenders were Meta's Instagram and Facebook online platforms, followed by other platforms such as TikTok, X, and YouTube. Among the affected were over 150 media outlets, indicating the harmful impact of this type of digital rights violation amidst genocide.

Additionally, a recent report by Human Rights Watch, "Meta's Broken Promises," underscored the extensive censorship of Palestinian voices by Meta at the height of the war on Gaza, which spanned over 60 countries¹⁸. The report documents over 1,050 instances of content removal and suppression on Instagram and Facebook from October to November 2023¹⁹. Among these cases, 1,049 involved peaceful pro-Palestinian content, while only one case involved pro-Israel content. In hundreds of cases documented by Human Rights Watch, comments such as "Free Palestine," "Ceasefire Now," and "Stop the Genocide," were repeatedly removed by Instagram and Facebook under "spam" Community Guidelines or Standards without appearing to take into account the context of these comments²⁰.

Across the span of the Israeli onslaught, Palestinian voices, especially those of journalists and human rights defenders, face significant and disproportionate censorship on Meta's social media platforms. This not only restricts freedom of expression but also hinders access to information. Meta's aggressive over-moderation of Palestine-related content

17. Charts, The Palestinian Observatory of Digital Rights Violations, data accessible at: www.7or7amleh.org

18. Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook, Human Rights Watch, December 21, 2023, Available at: www.hrw.org

19. Ibid

20. Ibid

has been a deliberate decision amidst ongoing atrocities. At the start of the war, Meta manipulated its content filters to apply stricter standards to content from Palestinians and pro-Palestinian rights advocates, compared to other regions and categories²¹. Normally, Meta would restrict content when its systems are 80% certain of a violation of the community guidelines. However, for Palestinians, this threshold was lowered to 25% as part of “temporary risk response measures.”²² 7amleh’s documentation and subsequent communications by Meta indicated that those temporary measures were not lifted, and that disproportionate and biased content moderation policies over Palestinian and pro-Palestinian content persisted.

The disproportionate over-moderation leads to restrictions limiting the reach of Palestinian content²³. In some cases, it can completely suspend users (including journalists, activists, and human rights defenders) on the platforms. Palestinian and international news outlets, including but not limited to Ajjyal Radio Network, 24FM, Modoweiss, as well as journalist accounts like Faten Elwan and Motaz Azaiza have all experienced and/or continue to experience content takedowns and account restrictions on Instagram and Facebook.

Another contributing factor to censorship are government requests for content takedowns on social media platforms, complicating the issue of transparency and bias in content moderation. Between October 7 and November 14, 2023, the Israeli Cyber Unit issued a total of 9,500 takedown requests to social media platforms, with 60% directed at Meta and a reported 94% compliance rate²⁴. This high level of compliance, combined with Meta’s lack of transparency in reporting these government requests, raises serious concerns about the undue influence of Israeli authorities on Meta’s content moderation policies. Without a transparent process to document and disclose these government requests, it remains challenging to verify the full scope of this issue within the wider problem of online censorship.

7amleh²⁵ and Human Rights Watch²⁶ have both identified systemic flaws in Meta’s policies, including overbroad enforcement of its Dangerous Organizations and Individuals policy and a heavy reliance on automated tools. Despite Meta’s commitments to address these issues, the company’s actions during the ongoing war on Gaza have only intensified the suppression of Palestinian voices, failing to meet human rights due diligence responsibilities.

21. Meta’s Ongoing Efforts Regarding the Israel-Hamas War, October 13 2023 (updated December 7, 2023), available at: www.about.fb.com

22. Schechner, S., Horwitz, J., Purnell, N., Inside Meta, Debate Over What’s Fair in Suppressing Comments in the Palestinian Territories, Wall Street Journal, 21 October 2023, available at: www.wsj.com

23. Briefing on The Palestinian Digital Rights Situation Since October 7th, 7amleh, 1 Nov 2023, available at: www.7amleh.org

24. Unjust Content Moderation at the Request of Israel’s Cyber, EFF, 26 July 2024, Available at: Unit www.eff.org

25. Hashtag Palestine 2023: Palestinian Digital Rights During War, 7amleh, 17 Jan 2024, Available at: www.7amleh.org

26. Meta’s Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook, Human Rights Watch, December 21, 2023, Available at: www.hrw.org

Furthermore, there were growing attempts to suppress speech critical of Israel during this time. In February 2024, Meta proposed revising its hate speech policy to equate the political ideology of “Zionism” with Jewish and/or Israeli identities²⁷. This would risk conflating legitimate political criticism of Zionism with antisemitism, stifling necessary political debate at a critical juncture. Beyond the troubling timing of this assault on Palestinians’ right to freedom of expression, 7amleh, along with 73 international civil society organizations, including Amnesty International and Jewish Voice for Peace, warned that this policy could mischaracterize discussions about Zionism, prevent Palestinians from sharing their experiences, and hinder efforts to combat real antisemitism²⁸. Moreover, a petition signed by over 52,000 people titled “Meta: We Need to Talk about Genocide” highlighted the importance of social media as a “lifeline [for Palestinians] during the Israeli government’s genocidal war on Gaza,” and that Palestinians should be able to name the political ideology impacting their survival without fearing reprisals²⁹. Despite the aforementioned opposition, Meta proceeded with a policy update on July 9, 2024, that will consider “Zionist” a protected category under its Hate Speech Policy³⁰.

Several online platforms also weigh the censorship of the phrase “From the river to the sea”, a slogan used frequently in protests against the ongoing aggression in Gaza and against Israeli policies in the occupied territories as a whole. In November 2023, Elon Musk went on X to say “decolonization” and “from the river to the sea” allegedly imply genocide, and using those phrases would “result in suspension” on X³¹. Similarly, Meta’s Oversight Board announced a review into the phrase “From the river to the sea” due to increased use post-October 7, 2023, amidst a debate about its meaning³². At the start of September, the Oversight Board ruled that the phrase “From the river to the sea” does not violate the platform’s policies on Hate Speech, Violence, and Incitement, allowing users to post it without risk of removal³³.

The broader trend of attempts to censor the phrase are not confined to social media. For instance, the US House of Representatives passed a resolution in April 2024 condemning the slogan as antisemitic, and the Dutch parliament followed with a motion declaring its use as criminal incitement to violence. These actions highlight a growing trend of attacks and restrictions aimed at undermining the rights to free expression and peaceful assembly, particularly of Palestinians and pro-Palestinian rights advocates amidst a bloody war.

27. Bhuiyan, J. and Paul, K., Meta’s review of hate speech policy sparks concern of further censorship of pro-Palestinian content, The Guardian, 10 February 2024, available at: www.theguardian.com

28. A Coalition of International Organizations Demands that Meta Refrain from Censoring Criticism Of Zionism on its Platforms, 11 February, 2024, Available at: www.7amleh.org

29. Petition: Meta: We Need to Talk about Genocide, Action Network, available at: www.actionnetwork.org

30. Update from the Policy Forum on our approach to ‘Zionist’ as a proxy for hate speech, Meta, July 9, 2024, available at: www.transparency.meta.com

31. Musk, E., X, 18 November 2023, Available at: www.x.com

32. Oversight Board Announces New Cases on Posts That Include “From the River to the Sea”, May 7, 2024, available at: www.oversightboard.com

33. New Decision Highlights Why Standalone Use of “From the River to the Sea” Should Not Lead to Content Removal, Oversight Board, September 4 2024, Available at: www.oversightboard.com

This censorship also reflects a pronounced anti-Palestinian bias. Online platforms are obligated to resist pressures to filter or censor political discourse, as stated in the Neutrality principle of the Internet Rights & Principles Coalition (IRPC) charter of human rights and principles for the internet³⁴. Allowing cultural hegemony can silence indigenous and marginalized voices, whose needs demand special attention. Social media companies are obligated by Article 19 of the UDHR to ensure everyone's right to express opinions without interference and to seek, receive, and transmit information and ideas through any media.

Harmful Content on Online Platforms

Hate Speech and Incitement to Genocide

On 27 October 2023, the United Nations Committee on the Elimination of Racial Discrimination expressed serious concern about “the sharp increase in racist hate speech and dehumanization directed at Palestinians since 7 October, particularly on the Internet and in social media.³⁵” It is evident from the mounting evidence and reports through the Palestinian Observatory for Digital Rights Violations (7or) that hate speech, incitement to violence, and dehumanization of Palestinians are already at an alarming level.

For instance, an online post on X from the Israeli Deputy Mayor of Jerusalem on December 8 described stripped and blindfolded Palestinian detainees in Gaza as “hundreds of ants” that he wanted to bury alive; “they are neither human beings nor human animals, they are sub-humans and that’s how it should be.³⁶” The post was removed after it was reported but many others remain. Such rhetoric continues to be commonly occurring across online platforms. It perpetuates the dehumanization of Palestinians and fuels an environment where violence is normalized and celebrated.

From October 7, 2023, to July 1, 2024, The Palestine Observatory of Digital Rights Violations (7or) documented 3,325 total violations for harmful content across major online platforms³⁷. The violations occurred mostly on Facebook, with 1,366 cases, and X, with 1,297 cases, with other cases occurring on Instagram, Telegram, and others. 73% of the cases are incitement, while the rest are spread between hate speech, smear campaigns, and other forms of harmful content.

34. the charter of human rights and principles for the internet, Internet Rights & Principles Coalition, August 2014, Available at: www.ohchr.org

35. Reuters, UN committee voices concern about rising Israeli hate speech against Palestinians, October 27, 2023, available at: www.reuters.com

36. King, A., Post on X, December 8 2023, screenshot available at: www.x.com

37. Charts, The Palestinian Observatory of Digital Rights Violations, data accessible at: www.7or7amleh.org

7amleh's Violence Indicator, an AI-powered Language Model that monitors the spread of hate speech and violence in Hebrew against Palestinians and their advocates on social media platforms, has counted nearly 8 million model-classified violent/hateful cases between October 2023 and July 2024³⁸. 76.5% of the cases occurred on X, in addition to 21.6% occurring on Facebook and 1.9% occurring on Telegram.

On 26 January 2024, when the International Court of Justice (ICJ) ordered provisional measures in the case of South Africa v. Israel, the Court adopted legally binding orders that include requiring Israel to prevent genocide against Palestinians in Gaza as well as to prevent and punish direct and public incitement to commit genocide, as foreseen in Article III(e) of the Convention on the Prevention and Punishment of the Crime of Genocide.

This ICJ order underscores the gravity of the situation, especially considering the documented use of online platforms to incite genocide against Palestinians in Gaza, including by the highest levels of the Israeli leadership³⁹. The ICJ took note of statements made by Isaac Herzog, President of Israel, and Israeli Defense Minister Yoav Gallant, and specifically referred to a post shared by the Israeli Foreign Minister Israel Katz on X, which read: "The line has been crossed. We will fight the terrorist organization Hamas and destroy it. All the civilian population in Gaza is ordered to leave immediately. We will win. They will not receive a drop of water or a single battery until they leave the world."⁴⁰

In the context of the war on Gaza, 7amleh detected nearly 3 million instances of violent content in Hebrew targeting Palestinians on X between October 6 and December 31⁴¹. This kind of incendiary content by the Israeli public, along with statements by senior Israeli government officials on X describing the Palestinian people as "human animals"⁴² and "children of darkness"⁴³, has translated into unlawful acts in Gaza.

38 Violence Indicator, The Palestinian Observatory of Digital Rights Violations, available at: www.7or.7amleh.org

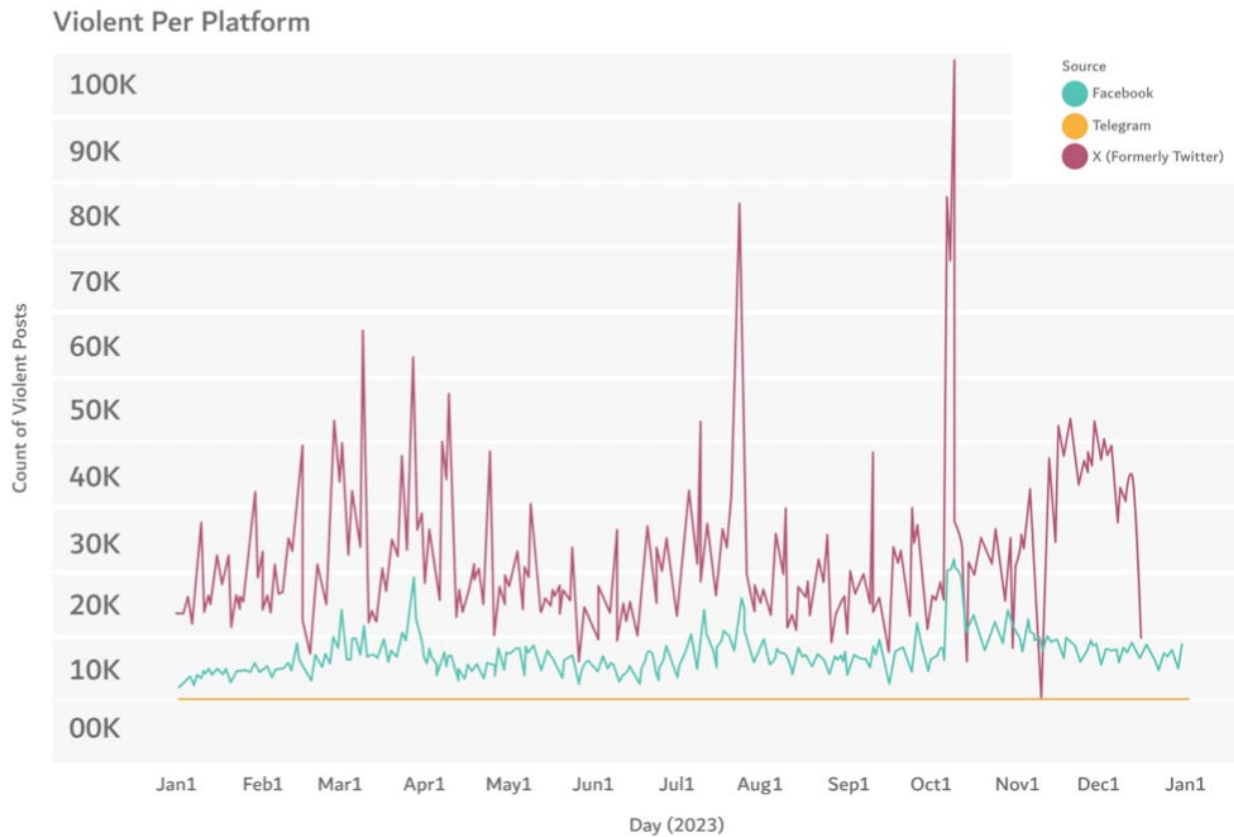
39. Law for Palestine Releases Database with 500+ Instances of Israeli Incitement to Genocide – Continuously Updated, available at: www.law4palestine.org

40. Katz, I, post on X, 13 October, 2023, available at: www.x.com

41. Position Paper Highlights Impacts of X Platform's Content Moderation Policies on Palestinian Digital Rights, 7amleh, 14 March 2024, Available at: www.7amleh.org

42. Gallant, Y., post on X, October 9, 2023, Available at: www.x.com

43. Sheth, S., *Netanyahu deleted a post on X about a struggle against 'children of darkness' around the time of a tragic hospital explosion in Gaza*, Business Insider, October 18 2024, available at: www.businessinsider.com



Telegram hosts several Hebrew-language channels with thousands or hundreds of thousands of subscribers which actively incite violence against Palestinian individuals, share and celebrate graphic content from Gaza, propagate widespread hate and dehumanizing speech. Despite several requests from civil society organizations, Telegram did not take action against any of those channels. For example, the channel “Terrorists from a different angle⁴⁴” has over 125,000 subscribers, and posts daily and celebrates extremely graphic footage of Palestinians killed or injured by the Israeli army in Gaza, including pictures of children captioned with dehumanizing language.

Addressing the transgressions by Telegram, the United Nations Working Group on Business and Human Rights sent a communication to both Telegram and to the UAE, where the company is based, expressing serious concern at Telegram being used as a conduit for human rights violations and abuses. The letter warned that in the “absence of preventive actions, regulations and sanctions, Telegram may continue to be used as a platform to disseminate disinformation, calls to violence, hate speech, and discrimination, amounting to violations of article 3 of the Universal Declaration of Human Rights (UDHR), which guarantees everyone’s right to life, liberty and security of the person.⁴⁵”

44. “Terrorists from another angle” Telegram Group, available at: t.me/dead_terrorists

45. UN Communication to United Arab Emirates, April 18 2024, available at: www.spcmmreports.ohchr.org

On February 7, 2024, the Palestinian Digital Rights Coalition sent letters to Meta, X, Telegram, and TikTok, urging them to address the proliferation of hate speech, dehumanization, and incitement to violence and genocide against Palestinians on their platforms⁴⁶. The coalition emphasized the documented use of these platforms to incite genocide, including by senior Israeli officials, and highlighted the ICJ’s concerns over genocidal rhetoric from Israeli leadership. Platforms always bear a significant responsibility to combat hate speech, this duty is especially critical amid the plausible genocide, drawing parallels to previous failures in Myanmar, where “Facebook’s algorithmic systems were supercharging the spread of harmful anti-Rohingya content in Myanmar⁴⁷” and in Ethiopia, where Meta “failed to adequately curb the spread of content advocating hatred and violence, this time targeting Tigrayans during the November 2020 to November 2022 armed conflict in northern Ethiopia.⁴⁸”

We note that online platforms have repeatedly failed to effectively combat anti-Palestinian hate speech and incitement on their platforms despite the magnitude of the human suffering the Palestinian people are currently going through. For example, after October 7, hate speech and incitement to violence targeting Palestinians spread rampantly across Meta’s platforms, but the company’s internal documents acknowledged then that the Hebrew hostile speech classifiers were not as effective as they should be, because they didn’t have enough data for the system to function adequately⁴⁹. The demand for Meta to establish effective hostile-language classifiers for Hebrew has been a primary demand by Palestinian and international digital and human rights organizations^{50 51}, and was a key policy recommendation in the 2022 Business for Social Responsibility report *Human Rights Due Diligence of Meta’s Impacts in Israel and Palestine*⁵².

Problematic Advertisements

Amidst the growing war on Gaza, some online platforms were found to be reaping financial benefit from disseminating harmful advertising content. 7amleh conducted an investigation into this matter, prompted by the discovery that Facebook ran targeted ads calling for the assassination of individuals, and ads calling for the forcible

46. Palestinian Digital Rights Coalition Demands Action from Online Platforms in Wake of ICJ Provisional Measures Order in Genocide Case, 7amleh, 7 February, 2024, available at: www.7amleh.org

47. Myanmar: Facebook’s systems promoted violence against Rohingya; Meta owes reparations, Amnesty International, 29 September 2022, Available at: www.amnesty.org

48. Ethiopia: Meta’s failures contributed to abuses against Tigrayan community during conflict in northern Ethiopia, Amnesty International, 31 October 2023, available at: www.amnesty.org

49. Schechner, S., Horwitz, J., Purnell, N., Inside Meta, Debate Over What’s Fair in Suppressing Comments in the Palestinian Territories, Wall Street Journal, 21 October 2023, available at: www.wsj.com

50. Meta: Let Palestine Speak www.meta.7amleh.org

51. Tell Meta: Stop Silencing Palestine www.stopsilencingpalestine.com

52. Human Rights Due Diligence of Meta’s Impacts in Israel and Palestine, BSR, September 22, 2024, available at: www.bsr.org

expulsion of Palestinians from the occupied West Bank to Jordan⁵³. The experiment, which tested whether ads that call for violence against Palestinians including calling for “holocaust for the Palestinians” and to wipe out “Gazan women and children and the elderly” would be approved, revealed that Meta failed to prohibit hate speech and incitement in paid advertising, inadvertently reaping financial benefits from the dissemination of harmful content within its platforms⁵⁴.

Additionally, a study by 7amleh has revealed that YouTube's ad policies fall short of complying with human rights standards, as demonstrated by their promotion of war advertisements without considering their long-term impact on Palestinians⁵⁵. Immediately after October 7th, the Israeli Foreign Ministry began producing and promoting videos as in-stream ads across YouTube, many of which contained graphic language and imagery related to Hamas. It is estimated that the Israeli Ministry of Foreign Affairs spent \$7.1 million on YouTube ads in the first ten days following October 7th, with almost all of that investment heavily targeting France, Germany and the United Kingdom⁵⁶.

Despite YouTube's policies against violent and graphic content, these ads were disseminated widely. Nearly 50 video ads in English were directed to EU countries, while viewers in the U.S. and the U.K. were pushed 10 and 13 ads, respectively⁵⁷. The ads included emotionally charged narratives, urging viewers to support Israeli actions in Gaza. This promotion of incendiary content without adequate moderation highlighted a significant gap in YouTube's adherence to human rights principles, as it not only breaches Google's guidelines but also undermines the dignity and rights of those affected by the war⁵⁸.

Disinformation and Influence Campaigns

Following the issues of censorship, hate, and incitement, disinformation on online platforms poses another significant challenge. It significantly impacts freedom of expression and access to information, as well as the right to security. This disinformation is employed to rationalize collective punishment against all Palestinians, and is often accompanied by incitement and calls for violence, escalating the danger for them both online and offline.

53. Biddle, S., Facebook Approved an Israeli Ad Calling for Assassination of Pro-Palestine Activist, The Intercept, November 21, 2023, available at: www.theintercept.com

54. Meta Should Stop Profiting from Hate, 21 November 2023, Available at: www.7amleh.org

55. Position Paper on Youtube's Impact on Palestinian Digital Rights during the War on Gaza, April 25, 2024, Available at: www.7amleh.org

56. Ibid

57. Israel floods social media to shape opinion around the war, Politico, 17 October 2023, Available at: www.politico.eu

58. Position Paper on Youtube's Impact on Palestinian Digital Rights during the War on Gaza, April 25, 2024, Available at: www.7amleh.org

In the context of the war in Gaza, disinformation not only misleads audiences but also critically disrupts humanitarian aid distribution efforts during a time when the whole Gaza Strip (2.15M people) face a high risk of Famine, high and catastrophic levels of acute food insecurity, according to the assessment by The Integrated Food Security Phase Classification (IPC), published June 2024⁵⁹.

This was exemplified by the exposure of the STOIC operation in Meta's Q1 2024 threat report, which also took place on other platforms besides Meta, including X and Youtube⁶⁰. This operation was orchestrated by Israel's Diaspora Affairs Ministry and run by a political campaigning firm called STOIC, based in Tel Aviv. It involved a coordinated network of fake accounts and websites that targeted audiences in the United States and Canada with pro-Israel content, particularly spreading disinformation against UNRWA before states took steps to defund the UN organisation at a time when it was the sole organisation managing the distribution of humanitarian aid in Gaza⁶¹. Despite efforts to conceal their activities, the network's use of artificial intelligence (AI) and inauthentic engagement was detected and dismantled by Meta and OpenAI, who also reported that they terminated accounts linked to the Israeli influence operation⁶².

An investigation by Haaretz revealed that the IDF Operations Directorate's Influencing Department, which is responsible for psychological warfare operations, created a Telegram channel called "72 Virgins – Uncensored" on October 9, which targets Israeli audiences⁶³. It shares graphic footage from Gaza dubbed as "exclusive content" and asks its followers to share their content widely so "everyone can see that we're screwing them." One message sent on October 11 reads: "Burning their mother ... You won't believe the video we got! You can hear the crunch of their bones. We'll upload it right away, get ready." Images of Palestinian captives and the bodies of alleged Hamas militants were captioned as "Exterminating the roaches ... exterminating the Hamas rats. ... Share this beauty."

The Israeli government's information warfare in Gaza is a product of a decade-long effort to dominate the narrative around its military operations⁶⁴. Israel and its supporters have effectively used dis and misinformation on online platforms to discredit Palestinian voices and justify Israeli actions, often through coordinated and deceptive campaigns that involve the Israeli government and non-state organizations who enjoy close ties

59. GAZA STRIP: Risk of Famine as 495,000 people face catastrophic acute food insecurity (IPC Phase 5), The Integrated Food Security Phase Classification, June 25, 2024, available at: www.ipcinfo.org

60. Meta Adversarial Threat Report, First Quarter 2024, May, Available at: www.transparency.meta.com

61. Benjakob, O., *Israel Secretly Targeted American Lawmakers With Gaza War Influence Campaign*, Haaretz, June 5, 2024, available at: www.haaretz.com

62. Disrupting deceptive uses of AI by covert influence operations, OpenAI, 30 May 2024, www.openai.com

63. Graphic Videos and Incitement: How the IDF Is Misleading Israelis on Telegram, 12 December 2024, www.haaretz.com

64. Accorsi, A., *How Israel Mastered Information Warfare in Gaza*, Foreign Policy, March 11, 2024, available at: www.foreignpolicy.com

with the government and its agencies⁶⁵. This includes leveraging AI-powered tools to amplify pro-Israel narratives while creating an illusion of grassroots support⁶⁶.

The proliferation of hate speech, incitement to violence and disinformation hinders the enjoyment of a variety of human rights, including the rights to life (article 6 of the ICCPR), security of person, including bodily and mental integrity (article 9 of the ICCPR), the right to the highest attainable standard of physical and mental health (article 12 of the ICESCR), non-discrimination (article 2 of the ICCPR), honor and reputation (article 17 of the ICCPR), and to protection from propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law (article 19 of the ICCPR).

65. White, B., Delegitimizing Solidarity: Israel Smears Palestine Advocacy as Anti-Semitic, *Journal of Palestine Studies*, Vol.49 No. 2 - Winter 2020, at: www.palestine-studies.org

66. Accorsi, A., How Israel Mastered Information Warfare in Gaza, *Foreign Policy*, March 11, 2024, available at: www.foreignpolicy.com

Artificial Intelligence, Data, and Automation in War

In the introduction, this report stated we are living in an unprecedented time. Israel's devastating war on Gaza revealed how various technologies, including Artificial Intelligence (AI), mass data gathering, and automation have become a central feature in the ongoing aggression. It is indeed unprecedented as we document how modern technological advancements are employed to exacerbate human rights and digital rights violations at a mass scale, facilitating acts that may be classified as Genocide.

There are two areas which must be discussed in order to establish the relationship between Israel's actions in Gaza, and the role of big tech companies. On one hand, we will look at the Israeli army's deployment of Artificial Intelligence-assisted target-generating systems⁶⁷, autonomous weapons⁶⁸, and extremely high levels of surveillance in Gaza⁶⁹. On the other hand, we will discuss big tech companies who operate cloud services in cooperation with the Israeli army⁷⁰ and Israeli weapons manufacturers⁷¹. Additionally, we will look at companies who inadvertently aid in Israel's harvesting of mass data due to a lack of safeguards to the right to privacy of vulnerable and at-risk Palestinian users, despite warnings to how data could be exploited to perpetrate violations of international humanitarian law⁷².

In November 2023, the United States organized a Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, endorsed by 50 states as of February 2024, notably with the US's key ally, Israel, not endorsing the declaration⁷³. The declaration stated that military use of AI must be ethical, responsible, and must comply with international humanitarian law (IHL), adding that "a principled approach to the military use of AI should include careful consideration of risks and benefits, and it should also minimize unintended bias and accidents."⁷⁴

Not only are advanced technologies facilitating systematic human rights abuses, but they also reduce human oversight, leading to indiscriminate killings and the violation of international humanitarian law at an exponential level. Big tech companies, whether knowingly or inadvertently, could be implicated in the ongoing atrocities by supplying tools, data, and/or infrastructure that enables the operation of those technologies.

67. Abraham, Y., 'Lavender': The AI machine directing Israel's bombing spree in Gaza, 972Mag, 3 April 2024, available at: www.972mag.com

68. Gaza: Israel systematically uses quadcopters to kill Palestinians from a close distance, EuroMed Monitor, 19 February 2024, available at: www.reliefweb.int

69. Frenkel, S., Israel Deploys Expansive Facial Recognition Program in Gaza, New York Times, March 27, 2024, available at: www.nytimes.com

70. Haskins, C., The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military, Wired, 15 July, 2024, available: www.wired.com

71. Biddle, S. Israeli Weapons Firms Required to Buy Cloud Services From Google And Amazon, The Intercept, 1 May 2024, Available at: www.theintercept.com

72. Biddle, S., This Undisclosed WhatsApp Vulnerability Lets Governments See Who You Message, The Intercept, 22 May, 2024, Available at: www.theintercept.com

73. US Department of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, 9 November 2023, available at: www.state.gov

74. Ibid

This section will explore how AI, data gathering, surveillance and automation are interrelated, and how their deployment in the context of Gaza impacts Palestinian digital rights. It will also highlight the need for big-tech accountability and strict regulations to prevent the use and abuse of these technologies in committing international crimes and violations of the Genocide Convention.

Artificial Intelligence in War

During the ongoing war on Gaza, Israel deployed AI-powered target-generating systems, such as “Lavender” and “The Gospel (Habsora)”⁷⁵ to automate the generation of bombing or elimination targets in Gaza. The initial expose by +972 Magazine described the AI-powered targeting system as a “mass assassination factory.”⁷⁶ Israeli sources revealed that the Lavender system identified 37,000 potential targets based on intelligence, a process that led to the approval of killing large numbers of Palestinian civilians⁷⁷.

An additional target system called “Where’s Daddy?” was used specifically to track the targeted individuals’ family’s residences. The outputs of the aforementioned systems were thousands of Palestinians killed, most of them women and children or people who were not involved in the fighting⁷⁸. Sources from Israeli intelligence told +972 magazine that in the first two weeks of the war, “several thousand” targets were initially imputed into the targeting programs like “Where's Daddy?” The source added that in the end, “it was everyone [marked by Lavender].” The result of the AI program’s decisions is evidenced in the death toll of the first six weeks of the war: 14,800 Palestinians were killed in Gaza, including about 6,000 children and 4,000 women⁷⁹.

The AI systems, including “Lavender,” “The Gospel,” and “Where’s Daddy?” function by analyzing vast amounts of data to rapidly identify and categorize potential targets. Lavender, developed by the Israeli army’s Unit 8200, uses machine learning algorithms to mark people and put them on a kill list⁸⁰. Gospel focuses on identifying buildings and structures for attacks, while “Where’s Daddy?” was used specifically to track the targeted individuals and carry out bombings when they had entered their family’s residences⁸¹.

According to UN experts, the use of AI systems such as “Gospel” and “Lavender,” combined with lowered human oversight, has contributed to a massive death toll and

75. Abraham, Y., ‘A mass assassination factory’: Inside Israel’s calculated bombing of Gaza, 972Mag, 30 Nov 2023, Available at: www.972mag.com

76. Ibid

77. Abraham, Y., ‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza, 972Mag, 3 April 2024, available at: www.972mag.com

78. Ibid

79. Hostilities in the Gaza Strip and Israel | Flash Update #50, UNOCHA, 25 Nov 2023, available at: www.ochaopt.org

80. Abraham, Y., ‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza, 972Mag, 3 April 2024, available at: www.972mag.com

81. Ibid

extensive damage to civilian homes and services⁸². The aforementioned systematic and widespread destruction constitutes crimes against humanity, war crimes, and acts of genocide as described by the UN Special Rapporteur on the occupied Palestinian Territory, Ms. Francesca Albanese⁸³.

Surveillance and Facial Recognition Technologies in Gaza

The AI systems discussed herewith rely on data fed through Israel's ever-growing surveillance regime imposed upon Palestinians in the occupied territory. Previously, 7amleh issued a report titled "Israel's Surveillance Industry and Human Rights," which provides a detailed analysis of the Israeli mass surveillance industry and how it has a detrimental effect on Palestinian lives⁸⁴. The use of spyware, social media data gathering, and facial recognition surveillance systematically erode fundamental rights such as privacy, assembly, movement, and freedom of expression⁸⁵.

In Gaza, Israel's use of surveillance technology in Gaza has deepened its ability to control and monitor the Palestinian population. Those systems were deployed on Israeli military checkpoints inside Gaza, along major roads Palestinians were ordered to use to flee south⁸⁶. The goal according to an Israeli officer was to create a "hit list of people who participated in the October 7th attack."⁸⁷

The mass facial recognition program deployed in Gaza created a database of Palestinians without their knowledge or consent, using technology provided by the Israeli company 'Corsight' for example. The company boasted of its technology's ability to identify people even if less than 50 percent of their face is visible, but testimonies by Israeli soldiers to the New York times said those technologies were not always accurate and frequently wrongly flagged uninvolved civilians as wanted militants⁸⁸. The facial recognition program's inaccuracies illustrated the dangers and ethical violations of using such technologies in a war zone. The false positives lead to wrongful detentions and interrogations. They dehumanize Palestinians by treating them as mere data points, demonstrating how the invasion of privacy helps spread fear and trauma amongst a population enduring an unprecedented aggression and unimaginable human suffering.

82. OHCHR: Gaza: UN experts deplore use of purported AI to commit 'domicide' in Gaza, call for reparative approach to rebuilding, 15 April 2024, available at: www.ohchr.org

83. "Anatomy of a Genocide - Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967", Human Rights Council, 25 March, 2024, available at: www.ohchr.org

84. Israel's Surveillance Industry and Human Rights, 7amleh, December 2023, available at: www.7amleh.org

85. Ibid

86. Israel quietly rolled out a mass facial recognition program in the Gaza Strip, The Verge, 28 Mar 2024, Available at: www.theverge.com

87. Ibid

88. Frenkel, S., Israel Deploys Expansive Facial Recognition Program in Gaza, New York Times, March 27, 2024, available at: www.nytimes.com

Israel's use of extensive surveillance technologies on Palestinian civilians, even before October 7, is contravening international law. In a 2020 report by The International Committee of the Red Cross (ICRC), it stated that surveillance systems posed "potential humanitarian consequences" to civilian populations living under military occupation, namely "being targeted, arrested, facing ill-treatment... or suffering from psychological effects from the fear of being under surveillance."⁸⁹

Major violations to the right to privacy of Palestinians through Israel's expansive surveillance is now leading to the automation of killings in Gaza. The surveillance is so pervasive that even ordinary interactions become data points used to oppress and control, further exacerbating constant psychological distress and trauma.

The Automation of Killing

During the war on Gaza, the Israeli army has increasingly employed small drones or quadcopters to conduct direct attacks on Palestinians in Gaza, resulting in numerous deaths and injuries⁹⁰.

The drones, including models like the Matrice 600 and LANIUS, are highly mobile and versatile, equipped with machine guns and missiles⁹¹. These drones utilize sophisticated digital technologies and artificial intelligence (AI) to autonomously search buildings, track and identify individuals, and execute missions with minimal human intervention, marking a chilling escalation in the automation of killing.

A report from November 2023 indicated that these drones, equipped with rifles, were patrolling the perimeter of Gaza's hospitals, firing single bullets at individuals, as described by British-Palestinian surgeon Ghassan Abu Sitta⁹². Elbit Systems, an Israeli arms manufacturer, provides these quadcopter drones to the Israeli army, featuring the Bird of Prey tactical weapons platform⁹³. This system is partially informed by AI and is designed to be carried and operated by a single soldier. According to a February 2024 release by Elbit Systems, integrated autonomous target recognition (ATR) enables the drones to autonomously detect, classify, and track individuals, although human authorization is required to execute a strike⁹⁴.

89. Automating occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory, ICRC, December 2021, Available at www.international-review.icrc.org

90. Gaza: Israel systematically uses quadcopters to kill Palestinians from a close distance, EuroMed Monitor, 19 February 2024, available at: www.reliefweb.int

91. Ibid

92. 'Drone snipers' firing at targets around Gaza hospitals, says trapped British doctor, The Telegraph, 13 November 2023, Available at: www.telegraph.co.uk

93. Did IDF Lure and Shoot Palestinians Using Drones Playing Recordings of Crying Infants?, Snopes, 26 April 2024, Available at: www.snopes.com

94. New State-of-the-Art UAS to be Launched by Elbit Systems at Singapore Airshow 2024, Elbit Systems, 12 February 2024, Available at: www.elbitsystems.com

Euro-Med Human Rights Monitor has documented numerous incidents where these drones have directly targeted civilian⁹⁵, including children and elderly⁹⁶. These incidents are part of a broader pattern of premeditated killings carried out by drones, often targeting unarmed civilians in their homes, streets, and public spaces.

In addition to physical harm, these drones contribute to psychological warfare. Reports describe instances where Israeli drones played recordings of women and children screaming for help to lure people outside, exposing them to targeted strikes⁹⁷.

The psychological impact of these autonomous weapons is profound. The digital capabilities of these drones, coupled with their capacity for sudden, lethal strikes, create an atmosphere of perpetual fear and insecurity among the population in Gaza.

These actions not only constitute severe violations of international humanitarian law but also highlight the horrifying human rights implications of autonomous weapons. The deployment of digital and AI technologies in warfare underscore the critical intersection of digital rights and human rights, illustrating the urgent need for international regulations that protect and safeguard digital and human rights, especially during times of war.

The Role of Big Tech

Surveillance systems, AI technologies, and autonomous weapons rely heavily on vast amounts of data, which are often stored and processed in the cloud. Big tech companies can provide the necessary cloud services needed to process the sheer volume of data required for these technologies, facilitating everything from real-time surveillance to the deployment of autonomous weapons.

Without the support of cloud computing from tech companies like Google and Amazon, Israel would struggle to operate its extensive data-driven military technologies⁹⁸. Cloud services offer the scalability and computational power needed to handle the complex algorithms and large data flows integral to AI and surveillance systems. This collaboration highlights the potential complicity of big tech in enabling and supporting military operations that result in significant human rights violations. The following section will delve into the specific roles played by these companies and the implications of their involvement in Israel's military infrastructure.

95. Gaza: Israel systematically uses quadcopters to kill Palestinians from a close distance, EuroMed Monitor, 19 February 2024, available at: www.reliefweb.int

96. Israeli army expands its use of quadcopters to kill more Palestinian civilians, Euro-Med Human Rights Monitor, 4 June 2024, Available at: www.euromedmonitor.org

97. Killing on Autopilot: How Israeli Drones Decide Life and Death in Palestine, Gender IT, 18 July 2024: www.genderit.org

98. Sype, E. Big Tech terror: For Palestinians, AI apocalypse is already here, New Arab, 24 July, 2024, Available at: www.newarab.com

Google and Amazon's Project Nimbus

Amazon and Google, through Project Nimbus, have established a controversial collaboration with the Israeli army and the Israeli Ministry of Foreign Affairs through a \$1.2 billion cloud computing contract that is linked to facilitating the Israeli army's operations⁹⁹. The collaboration between the big tech companies and the Israeli military raises concerns about a profound invasion of Palestinian digital rights, particularly the right to privacy.

In February, at a conference dedicated to Project Nimbus, the head of Israel's National Cyber Directorate, Gaby Portnoy, was quoted by Israeli media as crediting the contract with helping Israel's military effort in Gaza following October 7. "Phenomenal things are happening in battle because of the Nimbus public cloud, things that are impactful for victory," Portnoy said, adding "and I will not share details."¹⁰⁰

Project Nimbus provides critical infrastructure that supports data storage, machine learning, and AI applications, the extent of which includes AI capabilities such as facial recognition and sentiment analysis¹⁰¹. Additionally, according to an Israeli government procurement document, two of Israel's leading state-owned weapons manufacturers, responsible for manufacturing drones, missiles, and other weapons Israel has used to bombard Gaza, have been required to use Amazon and Google for cloud computing needs¹⁰².

It was reported in Israeli media that, at the "IT for IDF" conference held in July 2024 in Rishon LeZion, Colonel Racheli Dembinski, head of MAMRAM (the Center of Computing and Information Systems), an IT unit of the Israeli Army, provided significant information on the military's expanded use of public cloud services during the ongoing war in Gaza¹⁰³. Colonel Dembinski highlighted the unprecedented demand for computing power that arose, particularly around October 27, 2023, when preparations for a large-scale ground invasion on Gaza led to system overloads. She revealed that to address these challenges, the military turned to Amazon Web Services (AWS), Google Cloud, and Microsoft¹⁰⁴. This shift was reportedly due to the extensive range of services these providers offer, including Big Data management and AI tools. This contradicts Google's previous statements which claim: "The Nimbus contract is for workloads running on our [Google's] commercial platform by Israeli government ministries such as finance,

99. Perrigo, B., Exclusive: Google Contract Shows Deal With Israel Defense Ministry, Time, 12 April 2024, Available at: www.time.com

100. Haskins, C., The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military, Wired, 15 July, 2024, available: www.wired.com

101. Ibid

102. Biddle, S. Israeli Weapons Firms Required to Buy Cloud Services From Google And Amazon, The Intercept, 1 May 2024, Available at: www.theintercept.com

103. מתחילת המלחמה: ממרים חוותה מעל 3 מיליארד ניסיונות תקיפה בסייבר, Israel PC Mag, 10 Jul 2024, Available: www.pc.co.il

104. Ibid

healthcare, transportation, and education. Our work is not directed at highly sensitive or classified military workloads relevant to weapons or intelligence services.¹⁰⁵

Furthermore, a recent investigation by +972 Magazine showed that the Israeli army's cooperation with Amazon Web Services (AWS) is particularly close, in that the cloud giant provides the Israeli army's intelligence directorate with a server farm which is used to store masses of intelligence data collected through extensive surveillance of Palestinians in Gaza¹⁰⁶. The investigation revealed this collaboration between AWS and the Israeli army enabled the processing and storage of billions of sensitive data which has been used to confirm aerial strikes, some of which have resulted in the deaths and injuries of Palestinian civilians¹⁰⁷.

Given the increase in human rights violations, such as extrajudicial killings and collective punishment in the occupied Palestinian territory, the use of advanced data analytics and cloud services by the Israeli army put the role of those major tech companies in the spotlight. Project Nimbus has sparked protests from employees within both Google and Amazon¹⁰⁸, who argue that their companies are complicit in Israel's military actions and systematic injustices against Palestinians¹⁰⁹. In response to protests, Google fired a total of 50 tech workers for protesting Project Nimbus¹¹⁰.

In addition to its involvement in Project Nimbus, Google has demonstrated its ongoing relationship with the Israeli army by sponsoring the "IT for IDF" conference¹¹¹. Held on July 10, 2024, in Rishon LeZion, this conference brought together global tech firms to support the Israeli army. Although Google's logo was removed from the sponsor list at the last minute, internal documents viewed by The Intercept confirmed that Google was initially a co-sponsor, highlighting its deepening ties with the military involved in violent aggression against Palestinians¹¹².

The implications of Google and Amazon's collaboration extends beyond immediate military applications, posing broader questions about the role of technology companies in Israel's ongoing aggression, and their responsibility towards upholding human rights.

105. Exclusive: Google Workers Revolt Over \$1.2 Billion Contract With Israel, Time, 8 April 2024, Available at: www.time.com

106. Abraham, Y., 'Order from Amazon': How tech giants are storing mass data for Israel's war, 972 Magazine, 4 August 2024, Available at: www.972mag.com

107. Ibid

108. Activists Disrupt Amazon Conference Over \$1.2 Billion Contract with Israel, Wired, 26 June 2024, Available at: www.wired.com

109. STATEMENT from Google workers organizing with the No Tech for Apartheid campaign on Google's firings of 50 total workers, Medium, 23 April 2024, Available at: www.medium.com

110. Ibid

111. Biddle, S., Google Planned to Sponsor IDF Conference That Now Denies Google Was Sponsor, The Intercept, 25 July 2024, Available at: www.theintercept.com

112. Ibid

Metadata and Safeguarding Right to Privacy

Meta's platforms in general, and WhatsApp in particular, has faced significant scrutiny over vulnerabilities that can be exploited by state actors such as Israel, inadvertently aiding Israel's ongoing war on Gaza. In a book published in May 2021, the head of the Israeli army's intelligence Unit 8200, Yossi Sarel, outlined a system similar to Lavender that relies on AI and machine-learning algorithms to identify potential targets, including how WhatsApp metadata is used to build a comprehensive database on Palestinians¹¹³. The book details how metadata, including WhatsApp group memberships and communication patterns, among "hundreds of thousands" of features, can be used to assign ratings to individuals, flagging them as potential militants¹¹⁴.

In March 2024, WhatsApp's internal security team issued a warning about a dangerous form of government surveillance, despite the app's powerful encryption. According to an internal threat assessment obtained by The Intercept, governments could bypass WhatsApp's encryption through "traffic analysis," a technique involving the monitoring of internet traffic to determine which users are communicating, their group memberships, and potentially their locations¹¹⁵.

WhatsApp's vulnerability poses a severe risk to at-risk populations, particularly Palestinians in Gaza. The assessment suggests that Meta must decide whether to prioritize the functionality of its chat app or the safety of a vulnerable segment of its users. When even encrypted communications can be leveraged to feed into AI-powered targeting systems, Meta employees expressed concern that the company's product and its inadequate response to the threat assessment might be placing innocent people in the Israeli army's crosshairs¹¹⁶.

While the violation of Palestinian digital rights by Meta was discussed extensively in the earlier section on the role of online platforms, Meta's disregard for internal warnings and insufficient safeguards for the digital rights of Palestinian users have contributed to the exploitation of WhatsApp's metadata by Israel, jeopardizing the safety of vulnerable Palestinian users. There must be robust protections and a reevaluation of the company's human rights obligations amidst the ongoing war on Gaza.

113. Davies, H. and McKernan B, Top Israeli spy chief exposes his true identity in online security lapse, The Guardian, 5 April 2024, Available at: www.theguardian.com

114. Abraham, Y., 'Lavender': The AI machine directing Israel's bombing spree in Gaza, 972Mag, 3 April 2024, available at: www.972mag.com

115. Biddle, S., This Undisclosed WhatsApp Vulnerability Lets Governments See Who You Message, The Intercept, 22 May, 2024, Available at: www.theintercept.com

116. Ibid

Internet and Telecommunication Blackouts as an Unlawful Method of Warfare

Telecommunications blackouts Amidst the Ongoing War on Gaza

During its ongoing military campaign against Gaza, which has been deemed as plausibly constituting genocide by the International Court of Justice¹¹⁷ Israel has continuously obstructed internet and telecommunication services crucial to the Palestinian population therein, including targeting vital telecommunication installations. In particular, Israeli authorities have weaponized access to the internet and other forms of telecommunications in Gaza, which endured at least 15 telecommunications blackouts since October 2023, according to statements by NetBlocks¹¹⁸ and the Palestinian Telecommunication Company¹¹⁹.

Of particular concern is the intentional and sometimes orchestrated disruption of internet access and communication channels, which not only violates Palestinian digital rights but also serves as a means to advance Israel's military campaign against Gaza. Such actions also exacerbate the already catastrophic humanitarian situation for the affected Palestinian population and hinder their ability to access vital information, communicate with others, and seek assistance in times of need.

Since as early as 8 October 2023, Gaza has experienced a significant decline in internet connectivity and disruptions in telecommunication services. This is primarily attributed to the deliberate targeting by Israel of civilian telecommunication infrastructure and telecommunication company staff; technical disruptions to services; completely cut off the supply of electricity to Gaza; and obstructed the entry of fuel supplies needed to operate telecommunication company generators.

On 9 October 2023, the Israeli Defense Minister, Yoav Gallant, announced that he ordered a complete siege on the Gaza Strip, adding, "There will be no electricity, no food, no fuel, everything is closed."¹²⁰ As a consequence of this, electricity hubs and telecommunication stations have been the subject of Israeli attacks, thereby threatening to shut off the strip from the outside world and create widespread panic.

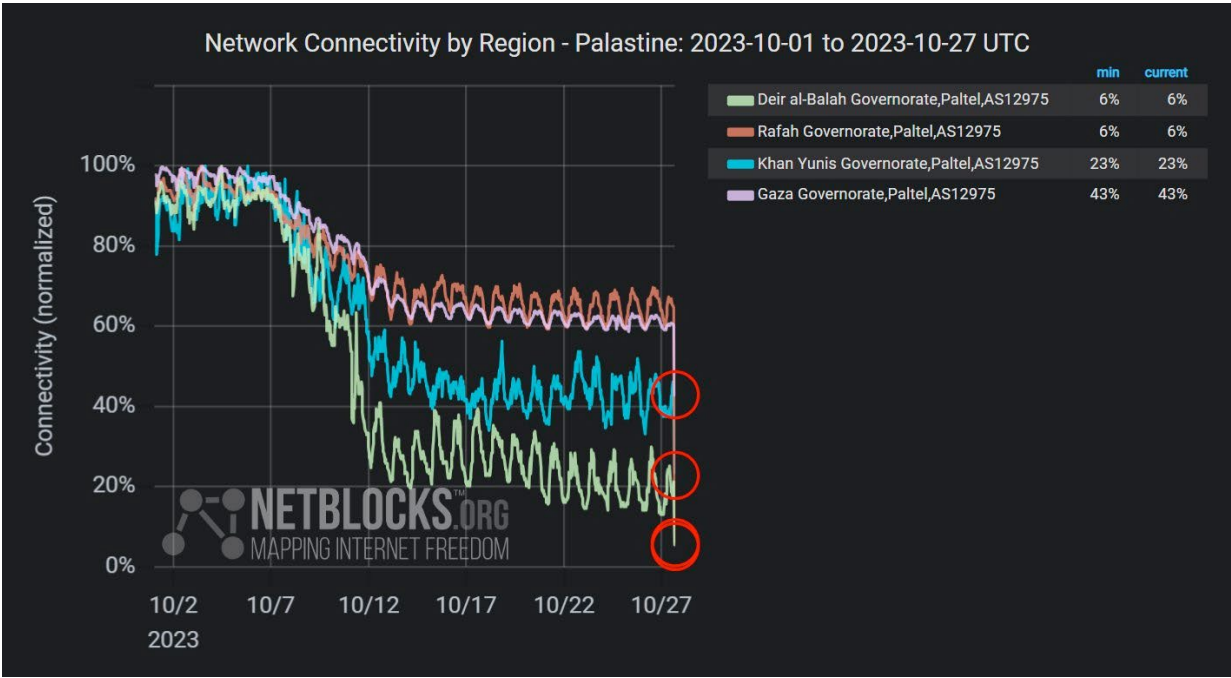
117. Order Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), International Court of Justice, 26 January, 2024, available at: www.icj-cij.org

118. Netblocks, official account on X, <https://twitter.com/netblocks>

119. Paltel Group, official account on X, <https://twitter.com/paltelco>

120. Fabian, E., *Defense minister announces 'complete siege' of Gaza: No power, food or fuel*, Times of Israel, October 9 2023, available at: www.timesofisrael.com

According to NetBlocks monitoring, since the beginning of Israel’s military campaign against Gaza, Palestinians went through at least 15 telecommunications blackouts spanning from 27-29 October, 31 October - 1 November, 5 - 6 November, 16-17 November, 4-5 December, 14-17 December, 20-21 December, 26-27 December, 12-19 January, 22-24 January, March 5, March 12, April 25, May 12, and May 25¹²¹.



Israeli airstrikes have either targeted or destroyed offices belonging to some Internet Service Providers (ISPs) operating in Gaza including Paltel and Jawwal in an outrageous display of disregard for International Humanitarian Law¹²². Rule 7 of the Customary Rules of International Humanitarian Law (IHL) mandates parties to a conflict to distinguish between civilian and military objects and forbids any attack on the former. Rules 11 and 12 further prohibit indiscriminate attacks which are not directed at a specific military objective, and which create no distinction between civilian and military objectives. Targeted infrastructural damage and direct attacks on telecom installations by Israeli forces have led to complete internet shutdowns that have directly affected civilians in Gaza and the West Bank¹²³. In addition, heavy bombardment from Israeli airstrikes has prompted incidental losses to the internet access and connectivity of 2.3 million residents of Gaza and contravenes the fundamental rule of proportionality as codified in Rule 14 of Customary IHL.

The deliberateness of Israel’s attempt to disenfranchise Palestinians from access to

121. Sourced from NetBlocks and Cloudflare Radar, live updates on X platform, last accessed 14 July, 2024, available at: www.x.com, and www.x.com
 122. Burgess, M., The Destruction of Gaza’s Internet is Complete, Wired, 27 October, 2023, Available at: www.wired.com
 123. Palestine unplugged: how Israel disrupts Gaza’s internet, Access Now, 10 November, 2023, Available at: www.accessnow.org

information is underscored by its targeting and killing of Palestinian workers who risked life and limb to repair the damaged telecom infrastructure¹²⁴. Although companies such as Paltel have devised tenacious means of keeping the Gaza population connected, such as burning cables deep into the ground, they are deprived of fuel by Israel. Paltel, whose joint office with Jawwal, was targeted by Israeli airstrikes¹²⁵, announced in November that it would go on a complete telecom blackout because its fuel reserves were exhausted¹²⁶.

Historical Context and Humanitarian Impact of Telecommunications Blackouts

Over the past decades, Israel has consistently prevented the development of self-sustaining telecommunication infrastructure in Palestine. Israel restricts the entry of essential technologies needed to run the telecommunication infrastructure in Gaza. Israel's clampdown on Palestine's infrastructure was further heightened in 2007 following Israel's unlawful closure and blockade on Gaza. Materials deemed as "dual use" are denied entry by Israeli authorities thereby limiting the operation of ISPs and curtailing the digital rights of the Palestinian people¹²⁷.

During periods of internet and telecommunication blackouts, the 2.3 million Palestinians in Gaza find themselves isolated from the rest of the world, unable to communicate with their loved ones or seek help. This leaves them in a perpetual state of terror, panic, and fear for their safety and the safety of their families. The blackout not only cuts off vital lines of communication but also hampers access to essential services, including medical and rescue teams. As a result, ambulances and civil defense teams face significant challenges in reaching injured civilians, leaving many trapped under rubble without access to urgent medical assistance. Conservative figures suggest there are more than 10,000 Palestinians trapped under the rubble, most of whom are presumably dead¹²⁸. During the blackout that persisted from January 12 to January 19, the Palestinian Ministry of Health in Gaza reported that Israeli attacks killed over 1,200 Palestinians.

Telecom shutdowns have significantly obstructed the delivery of humanitarian aid into and throughout Gaza. It has greatly affected the work of emergency health workers particularly from the World Health Organisation reported losing contact with its staff,

124. Telecom heroes risk life and limb under Israel's bombs, Al Jazeera, 21 November, 2023, available at: www.aljazeera.com

125. Post on X, October 9, 2023, Available at www.x.com

126. Gaza telecom companies warn of coming blackout amid Israeli attacks, Aljazeera, 15 November 2023, available at: www.aljazeera.com

127. Intensified restrictions on the entry of building materials delay the completion of housing projects in Gaza, UN OCHA, 13 Dec 2016, Available at: www.ochaopt.org

128. 10,000 people feared buried under the rubble in Gaza, UN News, 2 May 2024, available at: www.news.un.org

health facilities, as well as humanitarian partners on the ground amidst Israeli's aggravated bombing of feeder lines, towers and networks. The Director-General of the WHO, Tedros Adhanom Ghebreyesus, expressed concerns for the safety of humanitarian workers as well as the plight of patients in need of medical assistance amidst the telecommunications cut off¹²⁹.

Obstacles to Human Rights Documentation and Accountability

Telecommunication and internet blackouts pose a significant obstacle to documenting grievous human rights violations in Gaza for the purpose of accountability. This further underscores the correlation between severe human rights abuses and telecommunication blackouts. Without access to reliable communication channels and online documentation tools, it becomes challenging for human rights organizations to monitor, report, and hold accountable those responsible for violations against the Palestinian population. These blackout periods further obscure the truth and hinder efforts to ensure justice and accountability for human rights abuses in Gaza.

Indeed, telecommunication blackouts enable Israel to conceal the mass atrocities being committed against Palestinians in Gaza and to perpetuate its ongoing impunity. By severing communication channels, Israel restricts the flow of information from reaching the outside world, effectively controlling the narrative and minimizing international scrutiny of its actions. This deliberate suppression of communication not only shields Israel from accountability but also perpetuates the suffering of Palestinians by obstructing efforts to document and address human rights violations. Thus, telecommunication blackouts serve as a tool for Israel to maintain its dominance and evade accountability for its actions in Gaza.

Obstacles to Human Rights Documentation and Accountability

Telecommunication and internet blackouts pose a significant obstacle to documenting grievous human rights violations in Gaza for the purpose of accountability. This further underscores the correlation between severe human rights abuses and telecommunication blackouts. Without access to reliable communication channels and online documentation tools, it becomes challenging for human rights organizations to monitor, report, and hold accountable those responsible for violations against the Palestinian population. These blackout periods further obscure the truth and hinder efforts to ensure justice and accountability for human rights abuses in Gaza.

¹²⁹. WHO loses touch with staff, health workers in Gaza as telecommunications cut off, Middle East Monitor, 28 October 2023, available at: www.middleeastmonitor.com

Indeed, telecommunication blackouts enable Israel to conceal the mass atrocities being committed against Palestinians in Gaza and to perpetuate its ongoing impunity. By severing communication channels, Israel restricts the flow of information from reaching the outside world, effectively controlling the narrative and minimizing international scrutiny of its actions. This deliberate suppression of communication not only shields Israel from accountability but also perpetuates the suffering of Palestinians by obstructing efforts to document and address human rights violations. Thus, telecommunication blackouts serve as a tool for Israel to maintain its dominance and evade accountability for its actions in Gaza.

Violation of International Humanitarian Law

The Fourth Geneva Convention of 1949 codifies special protections for protected persons in occupied territory. Israel, as occupying power, is mandated under Article 55 of the Fourth Geneva Convention to ensure the provision of basic needs in the Occupied Palestine Territory, including the Gaza Strip. According to the International Committee of the Red Cross, the basic services necessary for the survival of the civilian population include electricity, health, water and telecommunications. These services require three components to function: people (e.g. service provider staff, telecom workers, repair engineers), hardware (e.g. mobile communication lines, telecom offices, generators) and consumables (e.g. fuel)¹³⁰. The three elements enable the functioning of the basic service system and are regarded as critical. The destruction of any of the above critical elements impacts the delivery of basic services necessary for the subsistence of civilians in armed conflict and is therefore prohibited under International Humanitarian Law.

The responsibility to “ensure the provision” of basic needs is a positive obligation, including the responsibility to protect digital rights in Gaza since access to basic needs and medical relief is incidental to the right of millions of innocent Palestinians to communicate while under siege in the Gaza Strip. Internet services play an important role in the work of emergency health workers, provision of assistance, and communication between families and humanitarian relief workers. The deliberate attacks on essential communication networks by Israel have hindered civilians from accessing these basic necessities.

Article 33 of the Fourth Geneva Convention expressly forbids the collective penalties, terrorism and intimidation meted out by Israel on the digital rights and infrastructure of the entire civilian populace in Palestine. Israel’s destruction of civilian infrastructure

¹³⁰. ICRC 2015, Urban services during protracted armed conflict: a call for a better approach to assisting affected people, International Committee of the Red Cross, Geneva www.icrc.org

constitutes “collective punishment” as it arbitrarily targets the entire civilian population. On October 31, barely 3 weeks after Israel’s attacks on Gaza, 15 of the 19 Internet Service Providers (ISPs) had completely shut down creating widespread panic amongst the Palestinian populace¹³¹. Israel has engaged in a complete military siege of Gaza hereby depriving the civilian populace of food, water, medical supplies, fuel and this has been further exacerbated by attacks on telecom infrastructure aimed at creating widespread fear and panic amongst Palestinians in Gaza.

Israel used telecom blackouts as a weapon of war, and this is illegal. It is concerning that humanitarian workers and press organizations on the ground have been stifled and prevented in their work of ameliorating the unbearable plight of the Gaza population. Israel must be reminded and made to comply with its obligations under human rights and humanitarian law as access to information is a right both in the time of peace and in the situation of conflict.

131. Palestine unplugged: how Israel disrupts Gaza’s internet, Access Now, 10 November, 2023, Available at: www.accessnow.org

Recommendations

Above all else, there needs to be an immediate end to the continued war. For there to be substantial progress made in ensuring the protection of human and digital rights in the region, a permanent ceasefire leading to the prompt end of the ongoing war crimes and violence is a necessary prerequisite.

Subsequently, all duty-bearers, whether in the public or private sector, must actively collaborate to unequivocally put an end to the systemic and deliberate discriminatory online policies and practices against Palestinians and individuals advocating for Palestinian human rights on a global scale.

Big Tech, Online Platforms, & Telecommunications Companies:

All companies providing technology, telecommunication, or social media services in Israel and Palestine need to prioritize a comprehensive approach that genuinely mainstreams and safeguards human rights and addresses the root causes of discrimination against the community and narratives, in full transparency and in line with the United Nations Guiding Principles on Business and Human Rights. Obligations of due diligence, transparency and reevaluation of policies and practices.

All companies must commit to conducting independent human rights impact assessments, which must be made public. Furthermore, publications must provide timely solutions with the aim of ensuring company practices and policies are in adherence with the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the Universal Declaration of Human Rights (UDHR).

Additionally, as a good faith immediate next step, 7amleh calls for the following:

Commit to:

1. Streamlining the process for addressing digital violations reported by civil society actors, ensuring that every report is met with timely and well-founded responses.
2. Investing additional efforts and resources to prevent further harm and protect the rights and safety of both users of the platforms and other rights-holders, including hiring staff with regional, linguistic, and socio-political knowledge to ensure localized policy decisions, especially when it comes to content moderation, are done in a rights-respecting manner.
3. Meaningful and regularly scheduled engagement with Palestinian civil society and stakeholders, not only during escalation in hostilities.
4. Recurrent, comprehensive, and transparent due diligence exercises to evaluate the impact of platforms' content moderation and curation decisions on individual and collective digital rights in Israel/Palestine.
5. Fully implementing, within a transparent, clear and detailed timeframe, all recommendations made by independent human rights impact assessments.

Ensure:

1. Proportionality and accountability through due process as an additional safeguard to protect Palestinian digital rights.
2. Users are provided the chance to respond to content takedowns and are provided detailed and timely information of the reasoning behind decisions on content moderation.
3. Deleted content is kept for a proportional amount of time.
4. User data privacy is protected, and individual user data cannot be weaponized to put individuals, especially vulnerable populations, in harm's way.

Guarantee:

1. Non-discrimination and avoid "one-size-fits-all" policies and practices.
2. Respect for freedom of the press and recognition of the newsworthiness of content created by citizen journalists, and permit its presence on the platforms, even when it contains references to illicit organizations or graphic content, in order to ensure access to information.
3. Services provided to clients which include technologies with a known weaponized use case are not being used to facilitate, war crimes, crimes against humanity, or genocide.

Provide full transparency on:

1. The implementation of notice and takedown mechanisms.
2. Governmental (both legal and voluntary) requests for content removal, as well as requests for user data.
3. Transparency reporting on contracts with state actors, especially police and military, with clear accountability mechanisms for inappropriate usage of any technologies with a known military use case.
4. Transparency about where automation and machine learning algorithms are being used in the content moderation process, including complete data on whether the content was correctly moderated, as well as keywords and hate speech lexicon used for both Arabic and Hebrew languages.

International duty-bearers

1. Call on the international community and the United Nations to take immediate and effective measures to halt ongoing systematic infringements on Palestinian digital rights, and create accountability mechanisms for grave violations of Palestinian digital rights, such as the intentional targeting of internet and telecommunications infrastructure.
2. Urge the European Commission to ensure that online platform content moderation obligations, as set by the DSA, are evaluated in a non-discriminatory manner and systematically taking into consideration all the specifics of the context, in full compliance with the DSA requirements and spirit¹³².
3. Urge the European Commission to fix loopholes in its regulatory frameworks, such as the AI Act, which does not require any obligations for technologies sold outside of Europe¹³³, and to generally advocate for the enforcement of regulations and alternative measures to compel online platforms, big tech, and telecommunications companies to cease discriminatory practices against Palestinians.
4. Urge big tech, online platforms, and telecommunications companies to adhere to business and human rights principles, as well as international humanitarian law, during the development and implementation of their policies, with a specific emphasis on due diligence responsibilities, especially in times of crises.
5. Actively engage with civil society and various stakeholders to effectively address their concerns regarding the safeguarding and advancement of Palestinian digital rights.

132. Domínguez de Olazábal, I., Palestinian Digital Rights and the Extraterritorial Impact of the European Union's Digital Services Act, 7amleh, April 2024, Available at: www.7amleh.org

133. Abrougui, A., The European Union's AI Act and its Implications for Palestinian Digital Rights, 7amleh, July 2024, Available at: www.7amleh.org

Contact us:

info@7amleh.org | www.7amleh.org

Find us on social media: **7amleh**

