MIFTAH Policy Brief | May 20th, 2025

The Future of Warfare and Global Accountability

Executive Summary

The Israeli occupation of Palestinian territory is marked by the systematic violation of digital rights through state-sponsored surveillance, censorship, and structural digital inequality. These practices, including biometric surveillance, arbitrary arrests based on online activity, social media censorship, and denial of technological infrastructure, constitute a broader strategy of control that mirrors and reinforces the physical restrictions of occupation. The use of advanced surveillance technologies not only infringes on Palestinians' fundamental rights to privacy and freedom of expression, but also threatens global human rights norms through the international export of these technologies.

Key Issues

1. Censorship and Control of Online Expression

Palestinians face systematic censorship on major social media platforms like Facebook and Instagram, often driven by direct requests from Israeli authorities. The “Facebook Law” and vague anti-terrorism legislation is weaponized to criminalize online dissent and restrict freedom of expression, violating the right to free speech. This crackdown intensified dramatically following the onset of the genocide on the Gaza Strip in October 2023. Since then, Palestinian social media content has increasingly become grounds for detention, with Israeli authorities using it as a pretext to justify arrests under the 2016 Counter Terrorism Law. Administrative detention, already a common practice employed against Palestinians, has also been weaponized as a means to silence dissenting voices. Concurrently, Israel’s Minister of National Security, Itamar Ben Gvir, has established a specialized “anti-incitement on social media” unit tasked with monitoring and censoring Palestinian content and conducting targeted arrests.

2. Digital Surveillance and Physical Repression

Israel’s use of advanced surveillance, including biometric data collection and AI facial recognition, has real life physical implications such as arrest, restriction of movement, and even targeted killing. MIFTAH’s study researched four AI weapons that have been developed by Israel and used on Palestinians: **BlueWolf, Lavender, Where’s Daddy,** and **The Gospel**. These tools are used for a range of purposes including, monitoring population movement, assessing targets, and timing attacks. They do not distinguish between civilian and military targets, and do not take precautions to minimize harm to civilians. They also 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. 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.

3. Shrinking Civic Space and Targeting of Human Rights Defenders

Israel's digital repression has extended beyond surveillance to include targeted harassment of Palestinian human rights defenders, journalists, and activists. Organizations critical of Israeli policies face aggressive cyberattacks, phishing attempts, and spyware infiltration. Notably, spyware such as Pegasus, developed by NSO Group, has been used to monitor and intimidate key figures in civil society. Digital smear campaigns targeting female activists have also been documented, using personal images and fabricated content to intimidate and silence dissenters. This has particularly deterred women from participating in protests or public advocacy, resulting in a chilling effect on freedom of expression and assembly. Additionally, Israeli authorities have orchestrated mass reporting campaigns on social media, pressuring platforms to take down Palestinian content under the guise of security concerns. These coordinated efforts effectively stifle dissent, restrict civic space, and undermine the ability of Palestinians to mobilize online.

4. Structural Digital Discrimination

Palestinians are denied access to essential information and communication technology (ICT) infrastructure, such as 4G/5G services, while Israeli settlers benefit from full digital access. This structural digital apartheid reinforces existing inequalities and prevents Palestinians from participating fully in modern civic and economic life. Palestinians are denied building permits by Israel to install a *comprehensive* fiber line in the West Bank in areas close to illegal Israeli settlements. Furthermore, the internet must be supplied through Israeli companies, compromising data privacy. In the Gaza Strip, internet infrastructure has been deliberately targeted and destroyed. In addition, repair technicians are prevented from repairing damaged infrastructure. Israel deliberately targets repair technicians and their crews as they carry out repair missions to restore connectivity in Gaza. In order to carry out these repairs, telecommunication companies must receive safe passage from Israeli authorities, which is often not granted. However, crews have still been targeted even with Israeli approval for safe passage. There have been 15 telecommunications outages in the Gaza Strip between October 2023 and May 2024. These blackouts create widespread panic and anxiety among civilians and make the work of emergency responders, humanitarian aid organizations, and UN agencies difficult if not impossible.

5. Global Risk: Export of Repressive Technologies

Surveillance technologies tested on Palestinians are exported globally, often without regulation. This normalization of rights-abusing tools threatens to erode privacy and civil liberties worldwide, making the Palestinian context a global human rights concern. Israel has established itself as a leader in the cybersecurity and surveillance industry and is among the world's largest exporters of weapons, ranking eighth in 2024. Such technologies are often promoted as having been successfully tested on the Palestinian population in the context of Israel's long-standing occupation. Israel's surveillance technologies are exported and normalized through global security partnerships. Technologies include facial recognition, spyware (e.g., Pegasus), predictive policing tools, and AI-driven surveillance and monitoring systems. These are often tested in the oPt before being marketed globally.

Recommendations

1. Arms Embargo and Military Accountability:

- Impose a two-way arms embargo on Israel. States must immediately suspend all transfers of military items and associated services and assistance to Israel.
- Put an end to and denounce imports of arms and surveillance technology from Israel.
- Refrain from supporting military operations that violate international humanitarian law and issue formal statements against the use of surveillance and censorship technologies that target Palestinian civilians.

2. Digital Rights and Online Expression:

- Focus on digital rights as an integral part of human rights by publicly condemning digital repression and including digital rights violations in regular human rights reporting and advocacy.
- Engage with social media companies to ensure content moderation practices do not disproportionately silence Palestinians.
- Monitor and report on instances of content takedown and encourage the creation of independent appeals processes.
- Provide direct support to Palestinian digital rights organizations and legal aid groups defending online expression.

3. Accountability and Legal Prosecution:

- Enforce applicable international accountability mechanisms and support legal prosecution efforts cooperatively before the International Court of Justice, the International Criminal Court, and UN human rights mechanisms.
- Mobilize and support universal jurisdiction efforts.
- Advocate for international investigations into surveillance technology use in the oPt.

To read MIFTAH's full report, scan the QR code: