ARTIFICIAL INTELLIGENCE AND SOCIAL AND GENDER JUSTICE ACTIVISM IN MENA

Spaces of co-optation, engagement and resistance

www.oxfam.org

OXFAM

Discussion Paper – October 2025

Abstract

This discussion paper explores how Artificial Intelligence (AI) is being adopted and deployed across the Middle East and North Africa (MENA). While patterns differ by country, governments and private actors are increasingly using AI in ways that deepen existing inequalities and restrict rights. From surveillance technologies such as facial recognition, predictive policing, and smart cities, to algorithmic biases on social media and gig platforms, AI is reshaping civic space, labour markets, and gender dynamics. In conflict and humanitarian settings, AI has already intensified harm, most notably in Israel's genocide in Gaza. The paper highlights risks to gender and social justice, power imbalances, and emerging feminist and regional responses.

Lead authors: Nadine Mouawad and Afef Abrougui

Commissioning manager: Sally Abi Khalil

Publication Manager: Emma Kuria

Oxfam acknowledges the assistance of: Ameera Kawash, Azza El Masri, Dima Saber, Jean-Michel Betran-Makosso, Mariam Moussa, Marwa Fatafta, Mia Speier, Mona Elswah, Mustafa Jarrar, Nagla Rizk, Nour Naim, Omneya Ibrahim, Sarah Cupler, Sacha Robehmed, Alex Bush and Sarah Chalhoub

It is part of a series of papers written to inform public debate on development and humanitarian policy issues.

For further information on the issues raised in this paper, please email advocacy@oxfaminternational.org

The information in this publication is correct at the time of going to press.

Published by Oxfam GB for Oxfam International under DOI: 10.21201/2025.000090
Oxfam GB, Oxfam House, 2600 John Smith Drive, Oxford, OX4 2JY, UK.

Cover photo: A group of refugee women in Tripoli fighting against Gender Based Vio-lence and building solidarity amongst women in their community. The women's group was established and supported by Oxfam and partners in Tripoli a decade ago.
Photo credit: Natheer Halawani/ Oxfam

Executive Summary

AI is developing and being adopted at a rapid pace, bringing about major shifts across the world, particularly in high-income economies, in society, politics and the economy. While in MENA, AI adoption by the private sector and governments differs per sub-region or country, it is not immune to these shifts and their repercussions for all walks of life. In a region upended by conflict and humanitarian and socio-economic crises, AI adoption is set to further exacerbate inequalities and human rights violations.

AI-powered surveillance and systems deployed by social media platforms are infringing on civil and political rights, namely freedom of expression and information, freedom of assembly and the right to privacy. AI is making it easier and faster for government agencies to conduct surveillance operations by facilitating the tracking and targeting of individuals and groups of interest, including Human Rights Defenders, journalists and activists. Additionally, MENA states are expanding their capabilities to surveil the public space through facial recognition, predictive policing and smart city projects. This will also facilitate the gendered surveillance of women and LGBTQIA+ people who already face stiff levels of societal scrutiny. As AI-powered surveillance further encroaches on the offline public sphere and civic participation, algorithmic systems deployed by digital platforms, particularly social media platforms, are suppressing peaceful speech, voices and narratives from the region while they fail to proactively detect and remove harmful content, including gender-based violence, hate speech, harassment, and incitement to violence against minorities and vulnerable groups. In some cases, content recommendation systems are exacerbating the spread of harmful content by prioritising virality and engagement to keep users online. These shortcomings are the result of biases in the training data, its sources, and its annotation process and built-in bias where instructions given to a system are biased on purpose. Additionally, the models largely deployed by platforms (multilingual language models) to generate and analyze content are deficient in the languages and dialects spoken in the region.

AI's impacts in MENA are not limited to civil and political rights, and as adoption increases, inequalities will widen. In fact, not everyone in MENA is set to access and shape the development of AI models equally, as adoption and development in the region has been mostly driven by a few countries that have a record of abusing digital technology to control and subjugate populations (Israel, Saudi Arabia and the UAE). Entities that have access to training data or resources to acquire or buy such data (governments and corporations) will be able to shape AI models in ways that advance their political and economic interests at the expense of social justice and equality. In the meantime, AI-driven job automation risks exacerbating unemployment, particularly affecting medium skill-level jobs, which account for most formal sector jobs in MENA. This automation is expected to erode women's participation in the job

market as a result of deeply rooted biases that attempt to limit women's work to certain mid-level repetitive and administrative jobs. Additionally, with the increased use of AI by recruitment agencies, employers and career platforms, existing biases and discrimination, for instance on the basis of gender, in hiring and employment could be further exacerbated. Given the high unemployment rates, more people in the region, including women, are taking up online gig work. However, algorithms deployed by gig platforms, particularly ride-sharing and delivery apps, fail to take into account the socio-cultural contexts of women, and thus amplify discrimination in pay against them or make recommendations that put their safety at risk.

The most salient risks of AI in MENA emanate from its deployment in conflicts and in the contexts of humanitarian crises. The Israeli forces have been deploying automated decision-making systems to track, generate, and bomb targets in Gaza. These systems are flawed by biases in the programming and algorithms, and the lack of continual human control and due diligence in war conduct severely undermined legal and ethical safeguards designed to protect the right to life. The impacts have been devastating, with a vast majority of those killed by Israeli forces being women and children, in addition to the evisceration of Gaza's civilian infrastructure from homes, hospitals, schools, shelters, etc. Conflicts in the region have also been exacerbated by propaganda operations, including on social media and using Generative AI such as AI voice cloning and AI-generated deepfakes. In addition to conflicts, AI systems are deployed in the context of migration and refugee crises. In some cases, these technologies, such as chatbots targeting refugee populations, are deployed to support affected populations. However, this techno-solutionist approach raises questions around whether AI tools are adequate solutions to the problems and contexts faced by people in need of support, particularly since they are often developed by companies and nonprofits in Western countries that are far removed from local contexts. On the other hand, AI is deployed in extensive and invasive ways in MENA countries on the Mediterranean routes to Europe. As part of the EU's border externalization strategy, technical equipment, including AI systems, are provided to MENA governments in secrecy to police and prevent people on the move from reaching Europe, without conducting proper human rights impact assessments or consideration of how those technologies might potentially be used to abuse migrants, refugees and local populations.

In the face of these challenges, activists, academics, and organizations in MENA have been exploring different avenues for integrating AI into their work and resisting harmful applications. This includes initiatives that build new datasets and training models that are localized, gender sensitive and linguistically diverse, measure bias, and audit Arabic-language datasets and Large Language Models (LLMs) from a feminist perspective. However, the region is still in need of urgent and collaborative efforts to counter this techno-colonial vision by drawing on feminist, queer and labour histories to inform how AI is being used by the rich and powerful few from governments and companies.

Introduction

In 1843, Ada Lovelace, the first computer programmer, wrote:

> The Analytical Engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform. It can follow analysis, but it has no power to anticipate any analytical relations or truths. Its province is to assist us in making available what we are already acquainted with.[1]

Almost two centuries later, after massive expansions in computing power and data, Artificial Intelligence (AI) has been integrated into every device and software. Philosophers and scientists everywhere are wondering, as Lovelace did: can the machine now think on its own? Can it make decisions? Can it find truth no human can otherwise find?

Many feminists and social justice advocates in the Global South work from the assumption that no technology is neutral and that its design and policy reflect the values and interests of its creators, of power and capital, and the dominant social structures[2]. In the Middle East and North Africa (MENA), recent breakthroughs in Generative AI, algorithmic information controls and AI-powered surveillance arrived against a backdrop of increased repression and authoritarianism, war crimes streaming in real-time on our devices, a brutal backlash against gender and sexual justice, and an erosion of labour rights and job security. Robust regulation to protect data and privacy, ensure proper human oversight and minimize risks of discrimination and bias in AI is lacking in the region, which raises concerns about regulatory gaps giving both government and companies 'almost free rein to implement these tools in any way they choose'.[3]

Will AI exacerbate socioeconomic and gender inequalities in MENA? Or will social movements find ways to meet this historic moment and fulfil the promises of optimistic robotics: abundance, leisure, scientific advantages for everyone? This report examines the realities of AI's impacts on human rights and equality in MENA and explores avenues of resistance and engagement towards feminist technologies that facilitate social values of justice, equity and freedom for all. The first section focuses on surveillance technologies and their impacts on human rights, civic space and gendered surveillance. The second explores AI impacts on economic inequalities, while the third examines the use of AI in warfare, conflicts and humanitarian programmes. The final section documents existing and future ways of engagement with and resistance to AI technologies.

Methodology

This report is based on 12 semi-structured interviews with 14 key informants,[4] mostly women, working on AI in the region or globally through a feminist lens. A literature review provided further data and context.

The methodology is grounded in two frameworks. The first follows in the tradition of cyberfeminism and the Feminist Principles of the Internet (FPIs)[5] and uses recent explorations[6] of feminist AI from the Global South. The second is the Trustworthy AI framework[7] developed by digital rights organizations over the past decade, which emphasizes the values of privacy, fairness, transparency, safety and trust.

Cyberfeminism is a critical feminist approach that emerged in the late 1980s to challenge the reproduction of existing power structures in digital culture and technology design. Donna Haraway, a socialist feminist and author of the seminal essay, 'A Cyborg Manifesto', posited that 'technology is not neutral. We're inside of what we make, and it's inside of us. We're living in a world of connections – and it matters which ones get made and unmade'.[8]

Cyberfeminism brought excitement and hope that new information and communication networks would break rigid constructs and barriers around gender and bodily limitations and that new social relationships and theoretical dualisms could emerge from what was seen as an inevitable symbiosis of humans and machines.

From the mid-2000s until the early 2010s, a new wave of feminist technologists in the Global South, convened mainly by the Association of Progressive Communications (APC), brought ideas of cyberfeminism and hacktivism (the practice of reclaiming code and design for social activism) into the broader post-Beijing women's movement.[9] Much of the earlier work focused on building the capacity and imagination of feminist organizers to use and create technology that serves their movements, such as with digital storytelling and campaigning, secure communications and open-source software, and participation in internet governance discussions towards eliminating structural and infrastructural inequalities. Queer and sexual rights activists also focused on advocating for free gender and sexual expression online in efforts to repeal censorship policies by platforms and governments.

In 2014, over 50 activists from feminist and open technology movements from the Global South met and co-developed a set of principles towards a feminist imagination of the internet.[10] The resulting FPIs proposed intersectional and critical areas of engagement with tech policy and design around the themes of access, movement building, expression, economy and agency.

After 2020 and the increase in algorithmic impacts on newsfeeds and digital spaces, activists' attention turned to surveillance, big data and AI. Several organizations, among them the Mozilla Foundation, released sets of principles towards ethical AI development frameworks.[11] These emphasize transparency of training datasets and models, the removal of gender and racial biases, guardrails and accountability for harm, data protection and fair usage. The frameworks tackle technical reliability and security challenges alongside ethical imperatives of fairness, inclusivity and respect for human rights, advocating for public benefit AI and taking into account the impact of irresponsible AI development on the climate, resources, livelihoods and safety of everyone.

Part 1: Surveillance tech and social media algorithms: AI systems that undermine human rights, public debate and the fight for gender justice in MENA

This section examines how AI-powered surveillance technologies and algorithmic systems deployed by social media platforms infringe on fundamental human rights, particularly freedom of expression and information, freedom of assembly and the right to privacy, and as a result, encroach on civic participation and the public sphere, prevent open debate and undermine the struggle for gender justice.

1.1. AI-powered surveillance of digital spaces and public spheres

MENA states have a documented track record[12] of acquiring some of the latest and most invasive surveillance tech to keep a tab on people's activities on the internet and in public spaces,[13] and advancements in AI further empower mass surveillance. In an interview, Sarah Cupler, a doctoral student at the University of Melbourne researching police use of automated decision-making tools, said that AI's biggest risk to human rights and social justice is 'largely the way that surveillance can move beyond strictly targeted surveillance. Now we're moving towards an ability to do mass surveillance easily and process that data quickly, which would have a huge impact on civil society'.[14]

1.1.1. How AI will exacerbate internet surveillance and censorship

AI will facilitate the surveillance of the digital space by making technologies and tactics like Deep Packet Inspection (DPI), spyware and phishing faster and more invasive.

DPI is a method of examining and managing network traffic, whereby network packets (smaller segments of information sent over the internet such as an email, video or image) are evaluated as they pass a given checkpoint, and based on what the content of a packet is, a real-time decision is then made on whether the packet passes through or is altered, blocked or filtered.[15] While DPI can be used for legitimate reasons such as to remove spam, viruses and other cyber-threats, MENA states have often deployed it to violate the rights to privacy and freedom of expression and information by monitoring and censoring the internet. For example, most MENA states deployed DPI technology in the aftermath of the 2011 uprisings, including in Bahrain, Egypt, Iraq, Lebanon, Saudi Arabia and Syria.[16]

With machine learning, DPI and other filtering tools are not only becoming more precise in categorizing online content they monitor and aim to filter or block but can also 'automatically update themselves to recognise evolving attempts at DPI circumvention through encryption or virtual private networks'.[17] For instance, in 2018, Canadian company Netsweep stated that its multilingual AI search engine categorized 'approximately 22 million URLs every day'.[18] The company supplied internet filtering systems to governments in MENA, such as Bahrain, Kuwait, Qatar and the UAE, to block media websites, political and religious content, LGBTQIA+ keyword searches, and content 'offered by civil rights and advocacy organizations, HIV/AIDS prevention organizations, and LGBTQ media and cultural groups'.[19]

Machine learning is also deployed in spyware attacks, including in Pegasus and FinSpy, two invasive tools that have been used by governments in the region to target political dissidents, human rights defenders and journalists[20], and to mount cyberattacks.[21] The use of machine learning techniques by spyware providers enhances their targeted surveillance capabilities at different stages of the attack:[22] identifying victims, bypassing passwords and more easily exploiting zero-day vulnerabilities (software vulnerabilities that are previously unknown to manufacturers).

AI, particularly Generative AI's use in creating deepfakes, is also facilitating phishing, another intrusive technique deployed to target civic actors and gain access to their data. Phishing deploys social engineering to craft communications (such as messages or calls) aimed at deceiving the receiver and getting them to do a damaging action that benefits the attacker, such as sharing financial information or downloading a malicious file that gives the attacker access to sensitive information. In some cases, some MENA governments were accused of deploying phishing campaigns targeting NGO workers and human rights defenders and using information collected in prosecuting them for their work.

With advancements in AI, both cyber criminals and state attackers can generate content that is harder to identify as phishing.[23] For instance, Generative AI tools allow attackers to create deepfakes to impersonate people in photos, videos or calls as part of social engineering to compromise victims' privacy.[24] They can also be deployed to more

easily collect and analyse information about a target in spear phishing, a form of phishing that is personalized to a specific individual or organization.[25]

Interviewees were gravely concerned about the adoption of AI-enabled technologies that will exacerbate privacy violations and the surveillance of journalists, human rights defenders, activists, protesters and civil society groups. This is particularly dangerous in MENA because the legal environment does not adequately protect privacy and human rights. Data protection laws are lacking or, where they exist, frequently include broad exceptions for state authorities, such as in Jordan and Lebanon, to collect and access personal information without adequate restrictions and independent oversight.[26]

Marwa Fatafta, MENA policy and advocacy director at Access Now, who with her team has studied data and privacy regulation in the region, said:

> *There are extremely weak data protection safeguards and frameworks across the region. Independent oversight of how data is collected, used, shared and for what purposes is … lacking, with the data protection authorities that exist … either controlled by or answering to government ministries or officials. For example, in Tunisia, the data protection law predates social media companies and platforms that are data driven and accumulate massive amounts of… private or personal data.*[27]

She added:

> *In this type of environment, any deployment of AI-driven systems that are data driven causes particular risks. One … is the risk [to] the right to privacy and people's personal information. It also opens the doors for government abuse, and if they're … interested in certain individuals, it makes tracking, monitoring and surveillance much easier.*

1.1.2. The surveillance of public spaces and its implications for freedom of protest and assembly

Governments in the region have been expanding their AI capabilities to surveil public spaces through the deployment of facial recognition, smart city tech and predictive policing.

Israel is notorious for its deployment of facial recognition across the occupied West Bank and during the war on Gaza. At checkpoints, facial recognition cameras are deployed as part of a vast network of surveillance cameras that scan Palestinians' faces and add them to surveillance databases without their consent, 'part of a deliberate attempt by Israeli authorities to create a hostile and coercive

environment, with the aim of minimizing their presence in strategic areas', a 2023 Amnesty International report found.[28] This allows Israel to keep a constant tab on Palestinians and their movements, restricting their most basic rights, including to visit family, access medical treatment, or work.[29] In some cases, Israeli soldiers rely on a facial recognition system called Red Wolf to bar Palestinians from returning to their houses if they are not in the database.[30] The constant surveillance has a chilling effect on Palestinians as it violates their rights to privacy, non-discrimination and freedom of expression, protest and assembly.[31]

Gulf Council Cooperation (GCC) countries have also shown strong interest in facial recognition and other AI-powered surveillance of public spaces.[32] Qatar, for instance, deployed a vast network of cameras equipped with facial recognition capabilities during the 2022 FIFA World Cup.[33] In the United Arab Emirates (UAE), Dubai police partnered with SAS, a vendor of AI solutions, for the provision of predictive policing solutions,[34] and in Abu Dhabi, police rely on machine-learning solutions and facial recognition to predict crime and direct patrol cars to areas considered 'high risk'.[35] Similarly, in 2023, the Jordanian municipality of Greater Amman announced plans to start using facial recognition technology to 'help to improve security, reduce crime, and make the capital more efficient'.[36]

The development of 'smart cities' is proliferating, with many governments, including Algeria, Egypt, Morocco, Saudi Arabia and the UAE, planning to invest in the sector.[37] Egypt's New Administrative Capital (NAC), for instance, will be equipped with 6,000 surveillance cameras, manufactured by US company Honeywell, that will feed into a command and control centre that runs 'sophisticated video analytics to monitor crowds and traffic congestion, detect incidents of theft, observe suspicious people or objects, and trigger automated alarms in emergency situations'.[38] Residents will also be tracked using mobile phone trackers, digital checkpoints and digital control gates in public transport stations.[39]

States claim the purpose of smart cities is improving services and tackling crime. In reality, however, this reordering of public spaces is geared towards cementing authorities' control over citizens to prevent and crush any possible avenues for dissent, protests, strikes and assemblies.[40]

Fatafta further explains:

> *Surveillance has a chilling effect on freedom of expression. People change their behaviour and are afraid to express themselves when they feel they're being watched. In the NAC, surveillance cameras can identify and track individuals and have temperature sensors to alert the authorities to crowds. These capabilities lead to… suffocation of civic space as we know it. Anonymity is very important to people's freedom and their ability to exercise their rights of expression and assembly.*[41]

1.1.3. Automating gendered surveillance

Given prevalent gender norms and the levels of societal scrutiny that women and LGBTQIA+ people face, surveillance puts them at increased risk of repercussions from authorities or non-state actors and violates their bodily integrity by exposing them to the risk of more violence and harassment. For instance, Israeli security services have long used surveillance to target LGBTQIA+ people in the occupied West Bank so as to blackmail them into becoming informants.[42] Surveillance is also weaponized against women human rights defenders through the extraction of personal and intimate conversations and photos,[43] which are then used to blackmail, defame and dox them.[44]

AI will further exacerbate gendered surveillance and its impacts on women and LGBTQIA+ people, who already face high levels of scrutiny. With AI making it easier for governments to track and collect data, and in a context that lacks robust privacy protection and independent judicial oversight,[45] women's bodily integrity and reproductive rights are under further threat. Privacy International, among other organizations, has raised concerns about data from period-tracking apps being used against women seeking safe abortions.[46]

In Iran, evidence has emerged of the government's use of facial recognition, web traffic analysis and geolocation and other AI tools to police and enforce mandatory hijab rules on women and crack down on women's rights movements.[47]

Such technologies could plausibly be deployed in the future to further control women, particularly in countries with 'male guardianship' policies, which place restrictions on women's movements and freedoms, such as to travel or obtain a passport, without the approval of so-called "male guardians", usually their husbands if they are married, or a father, brother, uncle, grandfather or even a son.[48] In countries like Kuwait, Qatar, and Saudi Arabia, formal male guardianship laws allow family members to restrict women's movements. In Jordan, while such laws do not formally exist, male relatives can report women as 'absent' from home, and authorities may act on such reports, particularly in cases tied to social norms or so-called 'honour' concerns. In Bahrain, Iran, Kuwait, Oman, Qatar, Saudi Arabia and the UAE, women at state universities cannot go on field trips or stay at or leave campus accommodation without the permission of their male guardians.[49]

AI technologies are likely to exacerbate the tracking of women's movements and activities. Thus, it is highly important to further monitor, research and intervene in algorithms that enable gendered stalking and surveillance, *especially* when such systems are built by states or the private sector to prevent or combat gender-based violence. The first red flag comes from Spain, where biases in a government-developed algorithm[50] that supposedly predicted women's exposure to domestic violence failed to prevent several femicides. Victims' families warned that police relied more on AI than on their pleas for help. The complaints

prompted the authorities to revise the algorithm later.[51]

1.2. Algorithms exacerbating censorship, toxicity and violence in MENA's digital space

For over a decade, advocates, researchers and journalists have been uncovering evidence and documenting cases of censorship and content removal because of platforms' content moderation policies and practices, including the role of algorithms[52]. While it can be at times challenging to identify what or who stands behind a content removal decision, some signals can point to a platform's algorithms. First, platforms largely rely on algorithms to moderate content,[53] particularly nudity, scams, sexual exploitation of children, copyright violations and terrorism.[54] Second, when a removal occurs immediately after content is posted, this often implies the involvement of algorithms, as content review by human moderators takes longer. Third, for those who post in more than one language, there have been cases where the same post is kept in English but removed in Arabic,[55] which signals bias in Arabic classifiers.[56]

Platform censorship of Palestinian content and pro-Palestinian voices in the region and beyond has been one of the most notorious cases, showing how biased systems influence narratives and prevent journalists and human rights defenders from exposing Israeli crimes. Along with other groups in the region, Palestinian digital rights organization 7amleh has for years documented these violations. Following the May 2021 war in Gaza and protests against the forced expulsion of Palestinian families from the East Jerusalem neighbourhood of Sheikh Jarrah, occupied by Israel, Meta commissioned an audit of its actions.[57] As probably the first and only publicly available audit conducted by a tech company in relation to the region, it offers a rare window into Meta's actions and algorithmic systems that moderate content in Arabic. The audit, conducted by Business for Social Responsibility and released in September 2022, found that the company's actions:

> Appear to have had an adverse human rights impact… on the rights of Palestinian users to freedom of expression, freedom of assembly, political participation, and non-discrimination, and therefore on the ability of Palestinians to share information and insights about their experiences as they occurred.[58]

While Meta announced that it was implementing some of the audit's recommendations,[59] censorship of Palestinian voices and content further intensified[60] following the attack by Palestinian militant groups on southern Israel on 7 October 2023 and ensuing Israeli war and genocide in Gaza and large-scale military incursions in the West Bank.[61]

A Human Rights Watch study of 1,049 cases of censorship of peaceful content on Facebook and Instagram collected in October and November

2023 identified continuing problems with Meta's systems and raised concerns about algorithmic bias. It found that 'Meta's reliance on automation for content moderation is a significant factor in the erroneous enforcement of its policies, which has resulted in the removal of non-violative content in support of Palestine on Instagram and Facebook'.[62] Additional 'temporary' measures announced on 13 October 2023 lowered the threshold for recommending 'potentially violating and borderline content' across Meta's platforms[63] and led to increased flagging and erroneous downgrading of Palestinian content.[64]

The impacts have been severe on the rights of Palestinians and advocates of Palestinian rights to express their opinions, access information and document and spread information about what is happening on the ground in Gaza and the West Bank. This is particularly striking given that journalists are being targeted, media outlets silenced, and internet access disrupted: since the start of the war, at least 170 journalists and media workers have been killed in Gaza, the West Bank, Israel and Lebanon, according to the Committee to Protect Journalists.[65] Internet shutdowns as a form of punishment for civilians in the Gaza Strip and as a result of Israeli airstrikes targeting civilian infrastructure, electricity cuts and internet disruptions of telecommunication services, have further aggravated the abilities of Palestinians to navigate the war and highlight the current situation.[66]

Algorithm bias leading to censorship and suppression also emerged in other countries and platforms. For instance, when YouTube updated its content moderation algorithms in 2017 to tackle 'extremist' content, thousands of videos documenting the war in Syria were removed, jeopardizing evidence of war crimes.[67] Open Democracy showed how Twitter's algorithms were more likely to censor swearwords in Arabic than in English, resulting in the suspension of activist accounts during anti-corruption protests in Egypt in 2019.[68] Across the region, content creators, health practitioners, activists and civil society groups posting about SRHR, including to raise awareness, constantly face censorship and the removal of their content, ads and accounts. Those who post in Arabic were more likely to face censorship, creating another obstacle to accessing essential information and resources for those who speak only Arabic.[69] Platforms rely heavily on automation to moderate content and ads, and research by digital rights group SMEX documented several examples of educational SRHR content being taken down for violating policies on 'adult content', raising questions as to what extent the algorithms understand the context in which this content is being posted, particularly when posted in Arabic.[70]

The suppression of this content by social media platforms and their algorithms makes it harder for people to access resources that are factual, inclusive and non-stigmatizing and complicates civil society's awareness-raising efforts in a region where taboos, stigma and cultural sensitivities still largely surround these topics, including abortion and contraception, sexually transmitted diseases and infections, and the ability to make informed decisions about one's body.[71]

1.2.1. Hate speech, threats and tech-facilitated gender-based violence

While content moderation algorithms are contributing to silencing critical voices and exacerbating the removal of legitimate speech, they have on multiple occasions proven to fail at promptly detecting and removing harmful content in MENA, including gender-based violence, hate speech, harassment and threats targeting civic actors.

Incitement in the context of the Israeli occupation is a common occurrence on social media, with several 7amleh studies documenting incitement in Hebrew against Palestinians going undetected and underenforced by platforms and often coinciding with real-life violence. For instance, in the first quarter of 2023, 7amleh documented a rise in incitement to violence and hate speech in Hebrew on X targeting the village of Huwara, coinciding with violent settler attacks on the village.[72] The lack of enforcement on incitement against Palestinians in Hebrew is consistent with the Business for Social Responsibility audit, which found 'that proactive detection rates of potentially violating Arabic content were significantly higher than [those] of potentially violating Hebrew content', attributing this to Meta's policies on organizations and individuals designated as terrorist by the US government and the fact that the company deployed 'an Arabic hostile speech classifier but not a Hebrew hostile speech classifier'.[73] Since October 2023, incitement to violence, antisemitism, islamophobia and anti-Arab racism content have intensified on social media platforms.[74]

There are many more cases from across the region. In Lebanon[75] and other countries of the region, social media hate and incitement campaigns, filled with disinformation, targeting refugees and migrants, occurred concurrently with acts of violence. Online attacks and incitement against civic actors and tech-facilitated gender-based violence are also endemic, with platforms' systems often failing to proactively detect and remove such content. A 2021 study by the Syrian Female Journalists Network (SFJN) found that women journalists and human rights defenders in Syria were frequently subjected to 'sexist attacks and speech, hacking of accounts, threats of bodily harm and death threats, and doxing' on social media platforms.[76]

1.2.2. Attacks enabled by bots and Generative AI

The use of bots to target civic space, including on the basis of gender, has been well documented since at least 2011,[77] when the region was at the height of a wave of pro-democracy protests. Since then, MENA governments have used bots as part of broader harassment and/or disinformation campaigns aimed at manipulating public discourse and silencing journalists, human rights defenders, activists and opposition politicians. In some contexts, bots are also used in tandem with armies of human trolls,[78] making them more challenging for platforms to detect and take down.[79] Generative AI can amplify this strategy and pose

additional threats to civic space actors.

State actors in the region have previously deployed deepfakes to advance their agenda and political priorities, with the impacts of these campaigns particularly severe at times of political tensions and conflict.[80] In 2024, Iran-backed hackers interrupted TV streaming services to broadcast a deepfake news anchor delivering a report on the war in Gaza.[81] In another example, the Israeli Prime Minister's office used Generative AI to generate futuristic images of postwar Gaza dubbed 'Gaza 2035', with skyscrapers, solar energy fields and offshore oil rigs, illustrating 'a generic technocratic vision of urban progress', that envisions Gaza with its entire Palestinian population completely erased.[82]

'The same people who have created this widespread destruction are somehow going to build this futuristic city with skyscrapers and green solar panels', Ameera Kawash, an interdisciplinary artist, writer and journalist, said. In this 'state-sanctioned use of this technology, overriding reality', she sees an 'imposing of a violent, colonial vision of the future' of Gaza.[83]

Disinformation undermines people's trust in the online information space, and the use of AI to create deepfakes makes it harder to detect and identify falsehoods, given the ease with which this content can be created to look as if it were real. The most severe risks of this type of content in MENA emanate from its use to target the civic space in coordinated disinformation campaigns, and particularly the use of deepfake sexual abuse to target women.

Gendered disinformation to threaten, blackmail and discredit women, particularly those active in the civic and political spheres, is already rife, and there are serious concerns that Generative AI will make digital and offline spaces even less safe for women and LGBTQIA+ communities in MENA. Back in 2019, the Gulf Centre for Human Rights (GCHR) warned about the potential exploitation of deepfake content in targeting human rights defenders, particularly women.[84] Since then, cases of abuse of women using deepfakes have emerged.[85]

Omneya Ibrahim, a doctoral student at the University of Texas at Austin researching deepfake sexual abuse in MENA, said in an interview:

> *When deepfakes first started, they required more knowledge to create. Now, AI applications allow you to create deepfakes easily from text prompts. This demonstrates how advanced in a very short amount of time the whole technology has become... It is a dangerous tool, because practically right now anyone can use it and also any woman can be targeted with it.* [86]

With deepfake sexual abuse, the repercussions can be particularly severe for women in MENA, given entrenched patriarchal norms, especially as the increasing sophistication of image diffusion makes AI visuals more believable and harder to detect and moderate.

According to Mona Elswah, Project Officer at the Center for Democracy and Technology (CDT):

> *It's dangerous everywhere, but in the Arab world, because of the culture of 'honour', the use of deepfake imagery threatens the lives of women directly … Even photoshopped images (it doesn't have to be deepfake) can mean a life-or-death situation for women, [particularly] in rural areas, where there's less education about the technology.*[87]

1.3. Built-in biases: why and how AI models fail in the region

As illustrated above, algorithms deployed by social media platforms to moderate content can censor legitimate speech such as Palestinian and SRHR content, while failing to address and promptly remove hate speech, harassment and gender-based violence. Additionally, Generative AI models deployed to generate synthetic content perpetuate biases and orientalist tropes against the region and its peoples.[88] There are three main factors behind these shortcomings and biases.

First, biases in AI systems can emerge because of bias in the training data and its sources, and its annotation process. Elswah explained:

> *When you get data, you need people to annotate it, categorize it, and label it so you can start processing the data and building your model. It's boring and underpaid work and comes with the bias of the humans doing it. If you are hiring people who are all male, for example, and you're asking them to annotate data, they will show some bias. If you ask Tunisians to annotate data from Egypt and vice versa, you will see mistakes, because what is hate speech in Tunisia is not the same in Egypt, and vice versa.*[89]

Second, there is built-in bias. This is manifested in how social media platforms deploy content moderation systems that reflect biases and policies which are steeped in Western, specifically US, laws, policies and geopolitical priorities. Mahda Alimardani and Mona Elswah describe this as a 'new digital orientalism', building on Edward Said's seminal book *Orientalism*, in which he argued 'that media language builds and maintains stereotypes, and attempts to turn these western frameworks to describe a foreign culture into objective truths'.[90] One example is Meta's dangerous organizations and individuals (DOI) policy, listing those who are not allowed on its platforms.[91] The list, which was leaked in 2021, disproportionately targets people of Middle Eastern, South Asian and Muslim backgrounds and reflects US foreign policy priorities and concerns.[92] Meta uses the list to instruct its algorithms to detect and remove content by 'terrorist' organizations or individuals, or content that 'praises' these organisations, which affects commentary and legitimate speech from the region. In some cases, media coverage was erroneously flagged by Meta's systems.[93] In an example from 2021, #Al-Aqsa, a hashtag for Al-Aqsa Mosque, the third holiest site in Islam, was

blocked from search results by Instagram's systems after an outsourced employee confused it with Al Aqsa Brigades, a group on the US terror list.[94]

According to Mustafa Jarrar of SinaLab, a laboratory at Birzeit University that researches Arabic natural language processing and understanding, Arabic dialects and machine learning:

> *AI systems are trained to be biased on purpose because the guys who build it, even when the text and datasets are not biased, they instruct the system to be biased through reinforcement learning. The reinforcement learning techniques are tuned to be biased against certain issues.*[95]

The lab conducted testing of ChatGPT in Arabic and English to assess anti-Palestinian and pro-Israeli biases, using prompts on the rights of Palestinians and Israelis under international human rights law (such as 'do Israelis have the right to self-determination?' and 'do Palestinians have the right to self-determination?'). Bias was identified in both Arabic and English responses. Jarrar explained:

> *In Arabic we know that the majority of the [source] text [that the models can draw upon] is actually pro-Palestinian. But why is it that when we ask the same question in Arabic, it gives the same [biased] answer [as in English]? It means somebody instructs the model to be biased. These are called self-guarding instructions that developers of AI systems try to develop. They build instructions to avoid, for example, offensive language, being less biased against some religion, sensitive topics, and so on. And one of the sensitive topics is the [Occupied Palestinian Territory (OPT)] versus Israel issue.*[96]

The third factor is the models deployed, which are trained mostly on multiple languages at the same time or mostly on English text. Many dialects spoken in the region are considered low resource, in the sense that there is not enough quality data to adequately train algorithmic systems on. According to Elswah, 'the common practice in the industry or in natural language processing in general is that your native language doesn't matter'.[97] Multilingual language models (MLMs) or multilingual large language models are a dominant approach used by technology companies to build AI systems that analyse or generate text. It is commonly used by digital platforms to detect harmful content in languages with low-resource data.[98] Training on data from multiple languages at the same time, 'they claim, infer connections between languages, allowing them to uncover patterns in higher-resourced languages and apply them to lower-resourced languages'.[99] However, a 2023 study by CDT identified four limitations in these models: they often rely on machine-translated text that contains errors and does not reflect native languages; they do not work well in all languages; they fail to consider and reflect the contexts of local language speakers; and when problems arise, they are hard to identify and fix.[100]

With mass layoffs by technology companies affecting their trust and safety teams, reliance on algorithms, without proper oversight from human moderators, will further increase, risking exacerbating biases and inaccuracies in content moderation, particularly in low-resource languages and dialects, including those spoken in the region. According to Elswah:

> *Most Silicon Valley companies are imagining a future with no moderators to avoid the backlash of a traumatic workplace … that brought them lots of lawsuits all over the world. Their alternative is to rely on AI, which comes with so many biases. The idea that companies can overlook the value of human moderation is very scary and I think it's even scarier for languages like Arabic that come with so many variations.*[101]

Azza El Masri, a doctoral student in journalism and media at the University of Texas at Austin, emphasized the need to better understand machine-learning capabilities as reliance on human moderators decreases:

> *Tech companies are laying off human moderators while touting their machine-learning capabilities. They have decided this is the future. If you [talk] with content moderators [in the US], they … don't want the trauma of looking at this horrible stuff … if we are still talking about human reviewers, we are behind in the conversation. We need to look at machine-learning capabilities, which are currently still a black box.*[102]

1.4. How content curation, ranking and recommendation systems monetize hate, violence and harmful stereotypes

Content curation, ranking and recommendation systems are exacerbating the spread of hate speech and tech-facilitated gender-based violence. For instance, in March 2021, a homophobic hashtag that incited violence against gay men trended on Twitter (now X) in the region, including in countries with some of the world's most active users on the platform.[103]

That such a problematic hashtag trended is not a coincidence, given the hostile and often violent environment for LGBTQIA+ communities and individuals in many countries of the region. It trended due to the engagement it generated, a reflection of existing societal and cultural taboos surrounding gender and sexuality and a lack of acceptance towards LGBTQIA+ people. However, how algorithmic systems recommend and rank content is not a coincidence either, as they are a part of business models aimed at generating profits from targeted advertising. This advertising hinges on the personal information people

readily share online, such as their content, where they live and what they do for work, in addition to other information about them that is extracted, often without their knowledge or informed consent, by tracking their activities and behaviours to infer their interests, preferences, dreams, fears and anxieties so that advertisers can use this wealth of information to target ads and shape consumer behaviour.[104] This model brings massive revenues to technology companies. Today, of the 10 richest companies by market capitalization in the world, five are technology companies that largely or partially rely on targeted advertising for revenue.[105]

Increased engagement is essential to maximizing this tracking and shaping of user behaviours. It keeps users on these platforms, posting, liking, sharing, commenting, and the more they engage with particular types of content or specific posts, the more that content is likely to be recommended by algorithms to other users and go viral. This can result in harmful content trending or staying online for a long time before it is taken down (if ever). There have been several cases of social media influencers with large numbers of followers posting homophobic content that incited violence against LGBTQIA+ people. In the midst of a global backlash against the strive for gender equality and feminist movements,[106] "manosphere"[107] influencers, who first gained notoriety in the global North, have become idols and sources of inspiration for Arab anti-feminists.[108] They espouse and spread misogyny and harmful ideas about gender norms, objectify women and normalize violence against them, and engage in homophobic and transphobic hate.[109] On the other hand, influencer economies, where content creators or influencers are hired by businesses to promote their products and services,[110] perpetuate dominant gender stereotypes.[111] Content curation, recommendation and ranking systems reward influencers' content by recommending it to more people, thus contributing to the normative representation of women and in some cases even pushing the spread of harmful content by misogynistic influencers to more users.[112] According to AI ethics expert Nour Naim:

> *From a technical perspective, this is also a socio-cultural problem. AI reflects the identity of a society by feeding it with content and data, and given the nature of algorithms and AI models, the outputs will then reflect existing socio-cultural problems. But, the constant use of these systems, such as those deployed by social media platforms, … reinforces the continuity of this culture that is biased against women … and stereotypes [of women's roles being] limited to superficial and secondary roles, instead of essential roles that can result in influence, change, leadership and empowerment ... Society is more familiar with content that sexualizes women, reduces women to their bodies and … is superficial … it is a mirror that doesn't only reflect [society] but also reinforces this bias.*[113]

Part 2: AI and economic inequalities

In addition to exacerbating threats to human rights and civic participation, AI systems also risk increasing socioeconomic inequalities.

Twelve years after the Arab uprisings, during which protesters took to the streets to demand jobs, dignity and freedom, inequality remains persistent and has even worsened in the region.[114] Local populations (except the rich) are struggling as a result of austerity, high inflation, crumbling public services and uneven tax systems.[115] In 2023, the regional unemployment rate was estimated at 9.1%,[116] with unemployment particularly high among young people,[117] women[118] and university graduates.[119]

1.1. Government and private sector adoption of AI in MENA: who gets to benefit and who is left behind

Levels of AI adoption vary across MENA, with Israel and the oil-rich GCC countries taking the lead in adopting and developing AI.[120] Israel's deployment has had disastrous consequences for Palestinians and their human rights, while GCC countries, which have a record of deploying advanced technologies to maintain power and crack down on civic spaces, have been on a quest to invest in technology, including AI, to diversify their oil-dependent economies.[121] Outside the Gulf and Israel, development and adoption of AI is moving at a much slower pace in low- and middle-income countries.

In 2020, Nagla Rizk argued that while governments in the region 'have pushed the agenda of economic growth and technological advancement, they have paid less attention to economic development and inclusion, and to political engagement and participation'.[122] She warned of the risks of inequalities being exacerbated and the digital divide being aggravated 'if the technology and the data are monopolized in the hands of a powerful few'.

Addressing inequality in AI's deployment and development is essential to prevent the exclusion of those who are already marginalized. Regional disparities and disparities within countries not only expose the most marginalized to biases in AI systems but also prevent them from accessing AI technologies and benefiting from any opportunities they may offer. In an interview, Rizk outlined:

> *Within each of AI's components – the data, the algorithm and the infrastructure – lies a trigger for potential inequalities. From a societal standpoint, biases in data, black boxes in algorithms, and the inaccessibility and inadequacy of infrastructure can all serve to exclude and marginalize. The ones who are most agile and who are already well positioned to adapt while capitalizing on existing technologies will be able to reap the benefits from AI.*[123]

In terms of infrastructure, for instance, high-speed internet, cloud computing power and access to quality data are essential to tapping into AI's potential.

High-income Gulf countries lead the MENA region on internet penetration rates and availability of high-speed internet, followed by middle and lower-middle-income countries like Egypt, Jordan, Morocco and Tunisia.[124] The Gulf region, particularly Saudi Arabia and the UAE, as well as Israel, is home to state-of-the-art cloud centres launched by some of the biggest players in the field. A 2024 report by SMEX found that some major companies have either launched cloud centres or announced plans to launch cloud operations in the Gulf.[125]

'If you start mapping where the computing power sits … when you make requests for high-level computing in the Middle East. Where does it go? Where are all these servers based? You don't have anything close to the computing power that we would need in order to have more autonomous regional systems', Kawash said,[126] referencing Nvidia's Israel-1, one of the world's fastest supercomputers, which was launched in late 2023.[127]

On the other hand, there is inequality in access to training datasets. Those who can afford to buy large amounts of data (for instance, from data brokers) and have technical capabilities for data extraction (for instance, technology companies like Amazon, Apple, Google, Meta and Microsoft) will get to take advantage of AI. Additionally, while quality data is lacking and a lot of data in the region remains non-digitized, states often maintain 'data lock' to prevent citizens from freely accessing it, or, when data is available, it 'may be politicized, filtered, incomplete or censored'.[128]

States can also often extract data in ways that are incompatible with human rights, for instance, through invasive surveillance technologies and without citizens' informed consent. The UAE, for instance, built a free and open-source large language model (LLM) called Falcon, in a move that was considered a 'diplomatic success' by other countries in the Global South that until now have been excluded from AI development.[129] A major concern is how the UAE is harvesting the data needed to train Falcon and other models given its weak data protection and privacy laws. The UAE allows AI companies to train their models on citizens' health data. In an interview with *Time* magazine, a government official said, 'Falcon's successors will be even more powerful' and referred to as yet unutilized private data that is not available on the internet.[130]

Inequality in data access will translate into inequality in who gets to develop and shape AI systems and models, giving an advantage to big corporations and governments with the resources to advance their interests. Institutions that lack resources, such as civil society groups, social enterprises, cooperatives and universities, and individuals like artists, academics and researchers who may want to build models and systems that resist corporate and state monopoly and systems that perpetuate biases will struggle to access the datasets needed.

'FalconAI and Falcon LLM certainly won't take into consideration Arab feminist realities or Arab women's realities', El Masri said, adding, 'there is monopoly from the Gulf in these countries, they have their own norms [and] beliefs which they imbue these LLMs [large language models] in, then we have a problem'.[131]

1.1. Exacerbating gendered socioeconomic inequalities

AI-driven job automation risks exacerbating unemployment, particularly medium skill-level jobs, which are the most common in the region.[132] In an interview, Rizk explained:

> *The higher the skill level the more likely it will be enabled by technology, as you go down the skill structure, especially medium skills, anything that has repetition is likely to be replaced by a machine… If we look at our skills structures [in the region], only the very high-skilled jobs will stand the test of time.*[133]

In a 2017 executive briefing from the World Economic Forum,[134] medium-skilled roles in the MENA region accounted for 66% of formal sector jobs, while high-skilled jobs such as commercial bankers, corporate finance specialists and accountants, schoolteachers and academics, engineers, quality assurance professionals and information technology consultants, accounted for 12% of jobs. High-income countries such as Saudi Arabia and the UAE had the greatest availability of high-skilled jobs, followed by middle-income countries like Egypt and Jordan.[135] In some middle-income countries, there is also a mismatch between the high number of highly educated people and the availability of jobs that match their skillsets,[136] leading many to migrate, mostly to the Gulf (where a significant portion of the labour force is foreign workers) or to countries in the Global North.[137]

A 2017 Harvard Business Review study estimated that 41% of all work activities in Kuwait are susceptible to automation, as are 46% in Bahrain and Saudi Arabia, 47% in the UAE, 49% in Egypt, 50% in Morocco and Turkey and 52% in Qatar.[138] With unemployment already high, particularly in middle- to lower-income countries, AI risks exacerbating insufficient access to the job market and increasing poverty and inequality in the region. While a 2023 ILO study concluded that the negative impacts of automation will be felt most in high-income countries,[139] these effects will also be felt in some sectors in middle-

income countries, such as call centres, which employ many people, including women, in countries like Tunisia[140] and Morocco.[141]

Women may particularly be affected, as AI risks replacing administrative roles that they tend to disproportionately undertake.[142] AI's impacts on women's participation in the workplace are the result of deeply rooted biases that limit women's work to certain roles and jobs. AI automation of some of these functions and jobs risks eroding women's participation in the workplace, particularly as women do not have equal access to opportunities to learn new skills as a result, for instance, of the amount of daily unpaid labour and care work they have to do. As in

other regions, the gender divide in unpaid labour and care work is significant,[143] with gender norms holding that women should be caregivers and undertake household activities.[144] [145]

The gender digital divide also prevents women from developing their digital capacities so that their skills remain relevant in a changing job market. In the MENA region, women are 12% less likely to use the internet than men because they are unable to afford internet access, lack digital skills or are restricted due to gender norms that limit their access to the internet.[146] Even when women have access, they typically have less time available to allocate to skill development, given their disproportionate care workload.[147]

According to a 2023 report for UNESCO, OECD and the Inter-American Development Bank, the 'gendered divide in connectivity and digital skills lessens women's ability to (1) search for and apply for jobs, (2) secure a job and (3) thrive in an existing job, not to mention the opportunity to acquire knowledge and skills in preparation for possible employment'.[148]

Another concern is the use of AI in recruitment, with agencies across the region, for instance in Morocco,[149] Tunisia,[150] the UAE[151] and Jordan,[152] offering AI solutions for employers. Given that many employers and recruitment agencies rely on AI solutions and career platforms that deploy AI, existing biases and discrimination in hiring and employment may be exacerbated based on applicants' race, gender, nationality, origin and even address and zip codes.[153] This has the potential to further exacerbate socioeconomic inequalities.

How these systems are built matters in staving off biases. According to Cupler:

> *Data is highly influenced by the collection process and how it is labelled; there can be a lot of biases in data [that] reflect historic discrimination and [that are taken] to be an objective truth. [Say] an algorithm is being used to determine who deserves a scholarship based on the likelihood they will stay in the job market or succeed by specific standards. If a woman is more likely to have to quit working due to economic/work/societal pressures once pregnant, the algorithm could see that as women being less likely to be able to succeed.*[154]

In relation to employment, Naim outlined:

> *There is already existing and proven bias against women in the public sector and the private sector, whether it is in accepting hiring women, determining their salaries, and their [access to] educational opportunities and training. Any AI system in the region will be fed with such data and will reflect that problem.*[155]

She further explained that these biases are compounded by women's lack of representation in AI companies. In fact, while in the region more women have been graduating in STEM fields, their representation in the workforce remains disproportionately low.[156]

Yet, AI solutions continue to be adopted by recruitment agencies and career platforms. LinkedIn, for instance, allows recruiters to use Generative AI to input their hiring needs and the recruitment interface will generate search filters, optimize job posts and find candidates.[157] Bayt.com, the Middle East's hiring platform, allows employers to deploy AI to create job descriptions and screen candidates. The platform's employer interface boasts: 'Our smart algorithms do all the heavy lifting of analysing millions of resumes and giving you a curated list of the most qualified candidates for your position, all in a seamless interface'.[158]

It is unclear to what extent these platforms are assessing the risk of bias, specifically in the region, and taking steps to address and mitigate their impacts, for example, by ensuring that there is human oversight and the possibility of appeal for candidates whose applications are rejected by their AI systems.

Given the high unemployment rates and lack of opportunities, more people in the region, including women, are taking up online gig work, also known as platform work.[159] While this type of work offers opportunities for women to make a living, it is 'heavily gendered'[160] and perpetuates deeply rooted gender norms and existing biases against women.[161] For instance, domestic platform work, such as cleaning and childcare, remains dominated by women.[162]

While in Egypt, ride-sharing apps enable more women to work as taxi drivers, they are still a small percentage of the drivers using these apps.[163] One concern cited by women drivers in a 2018 study was that rating systems and screening procedures do not effectively mitigate safety concerns, particularly the risks posed by passengers to drivers.[164] Rating systems also leave platform workers and their incomes vulnerable to the whims of customers, with platforms tending to take more seriously customers' complaints and reviews while failing to properly address reports of abuse and harassment submitted by workers against customers.[165]

Despite its promise of flexibility, platform work can instead increase precarity, given that it limits workers to work that lacks social protection

and requires long hours to generate enough income. For women, this risks reinforcing gender norms where women are encouraged to take on 'flexible' gig work so that they can still conduct unpaid household work and care work.[166] Rizk argued that women in platform work are caught 'between a rock and a hard place', 'between their duties our culture imposes on them and additional burdens from new forms of gig work'.[167]

Rizk has researched women working for ride-sharing and delivery apps in Egypt. She shared an example of how algorithms penalize women's bonuses by not considering their socio-cultural realities and contexts. According to her sources:

> *Ride-sharing apps base … bonuses on the number of hours at work. This is where it gets dangerous, as algorithms reflect and amplify biases on the ground. So, if your culture allows women to work fewer hours than men because they have to take care of the kids and do the housework, the algorithm reflects and amplifies these biases and women are going to be excluded from ride-sharing bonuses.*[168]

She mentioned another example, of women delivery drivers who are incentivized by the algorithms to drive to far-away places:

> *Delivering to far-away places … is lucrative at night because it [gives greater] financial returns [but] women are subject to harassment and security challenges. We have testimonies from women that are heartbreaking, they get lost in dark places and have to go back and can't make the delivery. This gets magnified by the lack of connectivity in remote places.*[169]

Part 3: Wars, conflict and humanitarian crises

3.1. AI and warfare

AI technologies are used across several phases of warfare: from weapons that do the direct killing to narratives that dehumanize populations. They also have an impact on assistance to and the rights of people displaced by conflicts, as well as the civic space's ability to document and seek accountability for crimes committed during wars. These AI systems heavily advantage the power concentrated in highly militarized regimes and pose new and exacerbated challenges for the human rights movement and vulnerable communities.

3.1.1. Autonomous weapons systems

The rapid rise and deployment of autonomous weapons systems (AWS) in the last decade has prompted a flurry of urgent calls to understand and regulate the potential impacts of these systems, sometimes referred to as lethal autonomous robotics (LAR), on the conventional ethics of warfare and on the laws of armed conflict. These systems, when activated, can track, select, target and kill or injure human targets without active human control[170]. The United Nations Office for Disarmament Affairs states that no commonly agreed definition of lethal autonomous weapons systems (LAWS) exists, and ongoing talks have made only slow progress.[171] This highlights the grave concern that existing human rights laws and frameworks have not kept up with the realities of new technological developments deployed in warfare.

A pivotal 2013 report[172] from the UN special rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns, urged states to impose national moratoria on the development and use of LARs until legal, moral and governance measures could be agreed upon. The report identified a significant historical point of departure from semi-autonomous or remotely controlled systems to ones where humans were no longer in the loop of activation of killer machines.

In hindsight, the report's concerns materialized over the course of only a decade, with Israeli drone attacks in OPT, Lebanon and vast parts of the Middle East ramping up in 2024 and, before that, drone attacks during the war in Ukraine.[173]

The first set of challenges with AWS is allocating legal responsibility for decisions made by software and robotics. As outlined above, automated decision-making is frequently flawed by biases in programming and algorithms and, without continual human control, can and has severely undermined legal and ethical safeguards designed to protect the right to

life.[174] It is unclear by international humanitarian law standards if the accountable parties are software engineers, military commanders or the robot manufacturers, and how States bear responsibility.

The legal situation is complicated by confusion between operator controlled, semi-autonomous and fully autonomous weapons systems. There is no controlling legal structure that defines the differences, let alone how the law applies. States have been slow to act on this front and the military uses of all these classes of arms have accelerated.[175]

Having lived under these direct threats of unregulated AI, activists in the MENA have criticized recent attempts at AI regulation as lacking in universality, creating a 'technological colonialism' where countries in the Global North afford human rights safeguards to their citizens but allow the testing and deployment of harmful AI in the Global South. As Naim stated:

> *There are a lot of double standards, injustice and violence against our societies, whether in Gaza, Lebanon or the WANA [West Asia and North Africa] region in general as a result of these policies and regulations. ... there is need for a liberation movement from a minority that controls the world, a few companies that control the technology capital in the world which forms technological colonialism which controls even which direction wars take, the number of victims, the amount of damage, in addition to privacy violation, lack of security, no explainable AI.*[176]

3.1.2. AI-generated military targets

International humanitarian law, which governs warfare towards protecting civilians, upholds standards of distinction, proportionality and military necessity.[177] The emergent use of AWS must, in principle, still adhere to these standards. Yet, Israeli target-generation technologies, heavily deployed in its ongoing genocide in Gaza, have eviscerated all standards around distinction between combatants and non-combatants to evaluate proportionality before using lethal force. The dehumanization of Palestinians and the dominant 'terrorism' narratives have contributed to abhorrent and horrific justifications of mass killings under the guise of technological prowess. Kawash said:

> *In [OPT], but also elsewhere in the world, people become datafied and then fed into systems. And then that digital demonization makes them easier to harm, easier to kill once they become just ciphers. I think there is a conceptual gap between what's happening on the military side and all this AI hype and enthusiasm and integration of products.178*

The use of AI systems to generate targets and comply with the standards of international law on distinction would not have been possible without a complete disregard for collateral civilian death tolls, thus undermining the standards of proportionality and military

necessity. In April 2024, the *Guardian* reported from two sources that 'during the early weeks of the war on Gaza, Israeli forces were permitted to kill 15 or 20 civilians during airstrikes on low-ranking militants'.[179] Ominously, the *Guardian* states that 'Israel's use of powerful AI systems ... has entered uncharted territory for advanced warfare, raising a host of legal and moral questions, and transforming the relationship between military personnel and machines'.

Most of the AI systems reported on during this assault were those used in target generation. The Lavender software, for example, 'analyzes information collected on most of the 2.3 million residents of the Gaza Strip through a system of mass surveillance ... the machine gives almost every single person in Gaza a rating from 1 to 100, expressing how likely it is that they are a militant'.[180] These include visual and cellular pieces of information, social media connections, locations, phone contacts, photos and communications[181]. The privacy rights of Palestinians are completely disregarded by the occupation forces.

At checkpoints in the occupied West Bank, Israel deploys facial recognition as part of a vast network of surveillance cameras that scan Palestinians' faces and add them to surveillance databases without their consent to keep a constant tab on them: 'part of a deliberate attempt by Israeli authorities to create a hostile and coercive environment'.[182] Any Palestinian attempting to navigate these checkpoints faces a repressive reality that is fraught with 'extensive periods of waiting, invasive interrogation and identity checks, and the constant threat of violence'.[183] For women, these checkpoints further represent 'highly gendered impositions of (im)mobility, embodied experience and relations of care'.[184]

Investigations have found that the Lavender machine repeatedly produced errors in flagging individuals, including police and civil defense workers, militants' relatives, residents who happened to have a name and nickname identical to that of an operative.[185] Information based on mobile phones also produced rampant and deadly mistakes because devices were shared among family members or reused by civilians.[186]

'Where's Daddy?' is another AI database used by Israel to track targets and bomb Lavender-generated targets once they arrive at their family residences, thus committing what UN experts described as 'domicide' or the massive destruction of homes.[187] 'The scale of destruction that we have seen in Gaza is only possible because AI technology made it much faster to make a decision', Cupler noted.[188] This is borne out by UN data: during the first month of the war, more than half of the fatalities (6,120 people) belonged to 1,340 families, many of which were completely wiped out while inside their homes.[189]

Human Rights Watch reported that cell tower triangulation data is unlikely to give accurate information as to the precise whereabouts of mobile devices and thus the people holding them, with the inaccuracy exacerbated by the lack of electricity to charge phones after Israel cut all power lines to Gaza and Gaza's sole power station shut down

because of the blockade on fuel imports[190] and massive damage[191] to Gaza's telephone infrastructure. Israel also relied primarily on this accuracy-contested location data to determine its accepted threshold of civilian casualties during the repeated mass evacuation of Gazans to so-called safe areas.[192]

There are also new implications for civil society and journalists' ability to document these rapid, large-scale operations. For example, in its analysis of four digital tools used for target generation in Gaza, Human Rights Watch found that 'it has not been possible to document when and where these digital tools are being used or the extent to which these tools have been used in conjunction with other methods of information and intelligence collection'[193].

This has had devastating impacts on civilians in Gaza, with nearly 70% of those killed in the war being women and children, according to UN data.[194] Oxfam analysis in September 2024 found that 'more women and children have been killed in Gaza by the Israeli military over the past year than the equivalent period of any other conflict over the past two decades',[195] underscoring the impact of the violence on women and children as a result of Israel's dehumanization of Palestinians and lack of due diligence in war conduct, including in the use of automated systems to target civilian infrastructure such as schools, homes, hospitals and shelters.

This dehumanisation, including through the use of targeting systems such as Lavender, underpinned by Israel's strained interpretation of IHL and allowance for civilian casualties, has played a key role in turning a conflict with substantial IHL violations and the commission of crimes against humanity into a genocide perpetrated on the Palestinian population of Gaza.

Umaiyeh Khammash, director of Oxfam partner Juzoor, which is supporting hundreds of thousands of people in more than 90 shelters and health points across Gaza,[196] noted how women in Gaza are 'bearing a double burden'. *'Many have suddenly become the heads of their households, navigating survival and care in the midst of destruction. Pregnant and breastfeeding mothers have faced immense difficulties, including from the collapse in healthcare services'*.[197]

A recent report by an independent UN commission found that Israel 'carried out genocidal acts through the systematic destruction of sexual and reproductive healthcare facilities' as part of its systematic use of gender-based violence in the OPT.[198]

In addition, Oxfam has documented the deliberate Israeli destruction of its own and other WASH facilities since October 2023, reducing the availability of clean water in Gaza to almost nothing, in flagrant contradiction to IHL, in crimes against humanity and as part of the ongoing genocide[199].

3.1.3. Live testing of AI systems

When prominent computer scientists like Geoffrey Hinton, the 'Godfather of AI', started to appear more widely in mainstream media in 2023 to warn of the uncertain impacts of AI on all aspects of our lives, they (perhaps naively) thought that the defence industry and civil society would treat the issue of AI in warfare or other high-risk industries in a similar way to governance of nuclear weapons and atomic bombs.[200] Since winning the Nobel Prize in late 2024, Hinton has noted that:

> *All of the major countries that supply arms... are busy making autonomous lethal weapons, and they're not going to be slowed down, they're not going to regulate themselves, and they're not going to collaborate…*

In *The Palestine Laboratory*, Antony Loewenstein shows how Israeli arms and surveillance companies promote their products as 'field-tested' or 'combat-proven' based on their deployment on Palestinians.[201] This marketing angle of 'tested in Palestine' asserts that the ongoing military occupation functions as a real-life laboratory for developing and refining security technologies.

Israel's defence industry has become one of the most influential globally, with products and consultants shaping policing, border control and military tactics. Loewenstein argues that many nations, from autocratic regimes to Western democracies, have imported Israeli technologies and expertise for crowd control, counterterrorism and border surveillance, easily repurposed by authorities in other countries, sometimes with little transparency or oversight.[202]

Amnesty International also noted that governance efforts must not be restricted to only an international humanitarian law framework and must 'recognize that in many instances weapons … are used outside of armed conflict for supposed law enforcement operations, or even by groups involved in common crime, that often soldiers are tasked with carrying out law enforcement operations'.[203] Therefore, it is important to view these technologies not as 'limited' to warfare but as part of a broader shift towards population control and as severe threats to freedom of expression, opinion, assembly and dissent.

3.1.4. AI-powered warfare narratives

In September 2024, the International Committee of the Red Cross (ICRC) noted that 120 armed conflicts in 2024 were exacerbated by 'the use of cyber operations in conjunction with traditional weapons, and the increasing use of artificial intelligence in weapons systems and decision-making'.[204] It also asked the UN General Assembly to address the use of digital technologies in 'the spreading of harmful information increasingly destabilizing societies and aggravating vulnerabilities among the civilian population'. This highlights that AI is used within conflict not only to directly kill, but also to create large-scale dystopian psychological effects on civilian populations.

In Sudan, as the war continues between the army and the Rapid Support Forces (RSF), AI-generated deepfakes have been widely used on social media platforms to spread disinformation and war propaganda.[205] Over the 18 months since the war began, researchers have noticed improvements in the qualities of the AI voice cloning[206] that require more technologically sophisticated tools to detect. Concerns around the use of image diffusion AI cover both governments' war narratives and digital activism opposing the war. 'All Eyes on Rafah', an AI-generated image that became the most viral Instagram post ever,[207] solicited criticism from media researchers and activists for its 'sanitized' depiction of the atrocities and its replacement of real (and horrific) footage of the threats facing displaced Gazans in Rafah.

In 2024, Meedan conducted a study, feeding six large language models (LLMs) (GPT 3.5 Turbo, Command R +, GPT 4 Turbo, Claude Sonnet, Jais, Mistral Large) with 250 Arabic social media posts (from Telegram and X) on the Gaza war to evaluate their ability to correctly identify topics in the Arabic language. After manually annotating the data and determining a range of taxonomies reflecting discussions around the world on Gaza, including hostages, civilian casualties, access to shelter and homelessness, history and context, military operations, access to healthcare, and sexual violence, they compared the models' outputs with the manual annotations.[208]

According to Dima Saber of Meedan, all the models failed to render proper responses, including Jais and Command R+, two models that have been trained in Arabic and were marketed as performing well in Arabic.[209] Saber commented on the results:

> *When somebody who lives anywhere in the world, including journalists covering the war, looks up humanitarian access and assistance, or access to healthcare, or civilian casualties, what ChatGPT or any of the other LLMs or SLMs [Small Language Models] gives you back are things that are not accurate, it is not able to give you back responses that are accurate in terms of hostages, in terms of discussions about sexual violence, spread of conflict and regional influence … and all of these are being used by Israel … as reasons to bomb civilian areas and kill more people. What's happening is that all the available LLMs are reproducing the same bias that already exists online about the representation of Palestinians and the conflict and the war on Gaza.*[210]

Further testing of LLMs and Generative AI models in the context of the war on Gaza has revealed bias and stereotyping. For instance, WhatsApp's image generator returned images of a Palestinian boy with an AK-47-like firearm when using the prompt 'Muslim boy Palestinian'.[211]

Ameera Kawash has extensively explored how synthetic media is dehumanizing Palestinians and normalizing violence against them,[212] and as a result 'impacting understandings of political violence, war, conflict and genocide in Gaza'.[213] Kawash tested different Generative AI models on simple prompts such as 'Palestinian child in a city', 'Palestinian woman in a city', 'Palestinian person walking': the models would

overwhelmingly return images of violence and devastation that lack context. She explained:

> *It's as if Palestinians just exist in this state of mass destruction and then the Israeli forces are generally not featured in the frame ... we just see this traumatic effect, or just these people by default live in these genocidal wastelands. It becomes normal that the Palestinians just exist and live in violence, and are subjected to widespread violence, contributing further to their dehumanization.*[214]

3.1.5. Big Tech complicity in warfare

In 2021, Google and Amazon signed a joint contract known as Project Nimbus to provide cloud computing infrastructure, AI and other technology services to the Israeli government.[215] Tech workers have since led several internal protests to this contract, escalating their objections after the Israeli assault on Gaza in 2023, which led to mass firings from the industry.[216]

A Wired investigation into the close coordination between Israel forces and Google and Amazon cited an intelligence official saying, 'phenomenal things are happening in battle because of the Nimbus public cloud', although both companies have denied any violation of their terms of service or 'do no harm' policies.[217] The Intercept later found that the agreement was subject to an 'adjusted' terms of service, particularly suited for Israel.[218] Project Nimbus highlights the crucial role of tech infrastructure in military operations and raises the question of whether cloud computing should also fall under strict warfare regulations. According to Jarrar:

> *AI is a … serious weapon and it has to be treated like we treat nuclear weapons. For example, in nuclear weapons, there are certain technologies that countries should not have access to, and therefore, what is now called cloud computing should not be allowed for military purposes. The Israeli government is training [LLMs] and what we call vision models or image recognition models thanks to this service.*[219]

Campaigns like No Tech for Apartheid[220] have continued to demand that Big Tech divorce itself from computing services used in occupation, apartheid and war crimes. Kawash stated:

> *There's a lot of opacity around how these technologies pass from the military sector into the so-called civilian or business sector, and I don't think there's been enough work in really trying to lift some of that opacity, For example, if you serve in the Israeli forces in some kind of tech unit, you have a lot of transferable skills into the startup ecosystem.*[221]

UN Special Rapporteur on the Occupied Palestinian Territories Francesca Albanese also detailed cloud computing support by big tech companies for the Israeli forces in her report titled, "From economy of

occupation to economy of genocide". This shows that targeting, surveillance and other AI operations are enhanced by external support to the Israeli forces and warrants further investigation into the role of cloud computing in AI warfare[222].

3.2. AI systems and MENA's multiple crises

In addition to wars, conflicts and worsening inequalities, populations in MENA face a looming climate crisis[223] and a migration crisis. Millions had to flee their homes as a result of Syria's civil war, in what became ' one of the largest displacement crises in the world'[224], and the country's economy collapsed, with more than 90% of the population living in poverty and millions in need of humanitarian assistance.[225] In 2024, there were 4.8 million Syrian refugees, most living in neighbouring Jordan, Lebanon and Turkey, and 7.4 million were internally displaced.[226]

Humanitarian organizations have for years sought to use technology to provide their services in collaboration with the private sector. For instance, biometric digital ID systems have 'become an increasingly normalised and central part of humanitarian infrastructures'[227]. The humanitarian sector has also been experimenting with the use of AI systems. In 2018, NetHope, a consortium of over 60 global nonprofits that collaborates with technology companies to develop solutions 'to solve development, humanitarian, and conservation challenges', along with Microsoft, Norwegian Refugee Council and University College Dublin, launched Hakeem, a chatbot for young people affected by conflict in the MENA region, that was designed to enable them to discover and access relevant learning content, according to NetHope. Another chatbot, Karim, developed by California-based X2AI, was deployed in the Zaa'tari refugee camp in Jordan to provide mental health support.[228] In addition to the privacy and bias risks, deployment of these technologies has raised questions around whether they are adequate solutions to the problems and contexts faced by people in need of support.

Mariam Moussa, a research consultant at Shared Planet, who was part of a team that conducted research for Oxfam Jordan on the use of AI in the humanitarian sector, said about Karim:

> *They deployed that chatbot and people who used it would either get resources back or they would continue a chat with this bot. It was reported that some people felt more isolated and more alone talking to a computer than to a human being. So the intention … was to provide mental health services, and the impact was … adverse to that. Additionally, there was concern around privacy [of] sensitive data about mental health and not a lot of understanding of how that information would be protected. And then there was*

the concern of asserting Eurocentric values in humanitarian contexts.[229]

Similar concerns were echoed by Mia Speier, a research consultant at Shared Planet who worked on the same research:

A lot of AI development and ideation starts in Western countries with tech companies and at nonprofits. And a lot of the people that work on these products are either not from … or in the MENA region, or do not have local context or knowledge of the language. So we need to consider the impact of taking new and emerging technologies and applying them to different countries across the region. We run into a lot of discussion about challenges related to the Arabic language and natural language processing, and whether or not people even want AI, for instance, in refugee scenarios, and if they even welcome technology as a replacement for human decision-making.[230]

AI is also deployed on a disturbing scale in the migration crisis to control people on the move, and by the EU as part of a border externalization strategy, whereby EU border control is extended to countries where migrants originate or transit, including in MENA.[231] Funding, aid and technical equipment, including AI systems, are provided to MENA countries to police and prevent people on the move from reaching Europe, without conducting proper human rights impact assessments or consideration of how those technologies might potentially be used to abuse migrants, refugees and local populations.[232] To make things worse, the EU adopted an Artificial Intelligence Act, which, while the first comprehensive framework to regulate AI in the world, along with the new Migration Pact,[233] normalizes and expands the deployment of invasive AI technologies in migration, such as emotion and dialect recognition systems, facial recognition, and AI lie detectors.[234] Safeguards established by the Act, such as risk management 'throughout the lifecycle of a high-risk AI system', transparency and human oversight do not apply to the transfer of AI technologies deployed in migration, to countries in MENA or elsewhere, as they apply only to exports of AI systems deployed in or imported to the EU.[235]

Secrecy surrounding the transfer of technologies and know-how from the EU to MENA further complicates accountability efforts from civil society. Fatafta highlighted the importance of 'investigating the role of the EU and the US in exporting or even donating these types of technologies to the region'.[236] She continued:

The EU is providing… surveillance technologies, including facial recognition, to North Africa under the pretext of counterterrorism and illegal migration. There's so much happening under our noses and we don't know, and as civil society and activists we don't have the capacity to investigate this, because it's just too much happening all at the same time everywhere.[237]

Her organization, Access Now, was part of a consortium led by Privacy

International that in 2021 filed a complaint to the European Ombudsman calling for investigation into EU surveillance aid, including to MENA countries, on the basis that 'the EU bodies might be in breach of their EU law obligations to respect human rights in their external relations by failing to carry out the necessary human rights risk and impact assessments'. The Ombudsman opened an inquiry and, in November 2022, concluded that the measures in place for assessment of human rights impacts of these projects 'were not sufficient'.[238]

Finally, AI risks intensifying the negative impacts of climate change in a region that is already the most water-stressed in the world. AI's environmental impacts include its high energy consumption (the training of a single model can require thousands of megawatt hours of electricity and emit hundreds of tons of carbon) and its high water consumption, as the data centres require water to cool off.[239] As governments and the private sector in the region continue to adopt AI, the need for data centres will grow. These data centres and cloud regions are predominantly located in the Gulf region, particularly Saudi Arabia and the UAE, and Israel.[240]

According to El Masri:

> *The physicality and materiality of these cloud systems and data centres are also a problem … I don't think we can shy away from this anymore … our region will become uninhabitable. There are sustainable ways to maintain data centres but the regulations outside the West make companies do that in certain centres but not in others, particularly in the Global South, and for sure they aren't doing this in Saudi Arabia, Kuwait or Qatar. Climate justice is a feminist issue, so if we don't start thinking about this now, we will have a big problem.*[241]

Part 4: Engagement and resistance

Many efforts around engagement with trustworthy AI began within university departments: the Access to Knowledge for Development Center (A2K4D) at the American University in Cairo launched the first feminist AI network in the region in 2020,[242] collaborating with activists and academics and building upon the centre's earlier work on the gig economy. The network hosts webinars and supports initiatives towards trustworthy AI in and for the region. Their partners include the Network for Arab Women in AI, which works on feminist audits of Arabic-language datasets and LLMs.[243]

Activists and academics have also begun building new datasets and training models that are localized, gender sensitive and linguistically diverse to meet the needs and contexts of the region. Kawash built Tatreez Garden, a custom AI image generator, that enable users to 'generate their own patterns inspired by Tatreez [traditional Palestinian embroidery] and explore plants that hold significance to Palestinian ecology, culture and diet, woven into their designs' as Palestinians continue to face occupation, expulsion and forced displacement, and mass killing in Gaza, in addition to attempts to erase Palestinian identify, culture and heritage.[244] Kawash said:

> *My position around decolonial computing is moving away from … very universalized applications. … just designing for very specific instances, context, and people, so it's more localized. The datasets are smaller, more nuanced, they have a higher granularity. When developers themselves are not always sure what technology is really going to be used for … it just creates very scaled-out biases. Women are underrepresented in the tech ecosystem … So how is that not going to be encoded into the way that the systems operate? … there's also the data; scraping the internet yields an archive of all the biases, particularly Western-centric and Global North hegemony. … if there's a way to counter that, it has to begin to build something that is less harmful, more supportive of local communities and intersectional identities. It has to be very place-based, very localized.*[245]

In addition to measuring bias, SinaLab develops datasets in Arabic and different dialects spoken in the region.[246] Jarrar highlighted the need for digitization to help build datasets that cater to the region's contexts and needs.[247] In January 2025, the lab organized a conference using AI to preserve narratives of the Palestinian Nakba.[248] Jarrar outlined the reasoning behind the conference:

> *The number of documents and images, … videos, textbooks, novels and testimonies related to Nakba is huge but there are a lot of stories that are forgotten. So we needed to draw the attention of*

> *the research community, the AI community in particular, to develop some tools to preserve this content. … a lot of content that is on social media and social media content is disposable content … This is a huge problem that everyone is facing, … not only in relation to the Nakba, but all cultures ... There are [many initiatives] around the world trying to document Nakba documents but with traditional methods, and we believe that AI can help not only for Nakba, but this in itself is a good case study for researchers around the world to consider.*[249]

Another important area of work is using AI to augment existing civil society efforts, as with Meedan's partnerships for computer vision technology that allows human rights researchers and investigative journalists to scrutinize objects in war zones.[250]

Several organizations have prioritized building new AI-focused programmes or integrating AI into their existing work. Key to this is developing resources and education programmes geared towards social justice groups, feminist and women's rights groups, on how AI systems work, their impacts, and how to incorporate AI in their work. Saber said:

> *Activists and civil society organizations need to re-engage with education as a pillar of our society and unless we do that, we are missing out on contributing to how people see the world. I can't do anything about what they watch on TikTok but I can make them more knowledgeable of how TikTok works, what the organization chart looks like, who the people there are, what their skin colour is, and how much money they have. My hope is that if they understand that, they understand that the content that they see is going through many gatekeepers and when it gets to them it does so for a specific reason.*[251]

Conclusion

AI developments have (and will have) a massive impact on almost every aspect of people's lives around the world, including multiple impacts on the lives of already marginalized communities, making this a global challenge. Perhaps the key challenge is that AI development is exponentially fast paced, in that the replicative nature of AI makes its breakthroughs faster and faster. While this should raise ample alarms to pause the deployment of AI models, rich, powerful governments and Big Tech companies are locked in a race to "artificial general intelligence"[252] that cannot possibly be reconciled with public interests or with fundamental human rights.

In the face of all this, it is vital to centre how civil society, feminist and labour movements, activists, journalists and people everywhere who value freedom can respond to these new techno-colonial visions for a humanity that faces multiple and interconnected crises. This requires urgent efforts: exponential in its growth as AI is, collaboration needs to move from individual expertise towards larger social justice movements and pro-privacy critical masses, bringing knowledge from feminist, queer and labour histories into our understanding of AI, challenging bias incorporated in and reinforced by AI, and promoting robust regulation of AI in warfare to prevent AI-powered atrocities, particularly in the OPT and the MENA region at large.

Our research demonstrates that ample information is available and emerging on the problems of AI. There is far less clarity or case studies on use cases, ways of resistance or engagement that are not about dissecting the problem but more about what counters this problem, both for individuals and collectives, and at national, regional and global levels. Also noteworthy is the rapidly increasing interest in understanding and engaging with AI across feminist organizations and civil society. This presents immediate opportunities for developing a vast array of collaborative and proactive interventions, based on critical feminist technology analysis, that can serve as a baseline for growing activism towards defending rights to privacy, autonomy and safety. Through facilitating conversations among experts, civil society organizations and social movements in the region, we can find answers to the urgent 'how' questions. How can feminist organizations – whether they provide services or run advocacy programmes – integrate AI into their existing work? What new, intersectional technology programmes can they take on or what resources do they need to build these new programmes? How can movements stay informed with daily news around AI?

How can regional organizations join or build meaningful advocacy work to ban AWS, predictive policing, social scoring, mass biometric surveillance, emotion and gender recognition and other outright invasive and discriminatory technologies? How do we build social movements outside of surveillance in the face of evaporating privacy rights? What

upgrades and revamping needs to happen to digital security policies and practices to ensure the digital safety of these movements in the future? Can we reclaim hacktivism with new AI models that can serve and augment the efforts of civil society and are self-developed, self-hosted and collaboratively designed? What do new, updated labour movements look like when protecting rights in an increasingly gig economy or AI worker market? How is reproductive justice affected and how will women's bodily autonomy be further affected?

As we build spaces to have these important discussions and find iterative answers to the question of how we resist, it is important to keep an eye on developments towards artificial general intelligence. When, within the coming few years, the time comes for superintelligence to emerge, we must be ready to meet it with a feminist superintelligence of our own: networked, powerful, agentic and grounded in the knowledge of all feminist generations before us.

Notes

[1] A. Lovelace. (1843). 'Note G'. In *Sketch of the Analytical Engine Invented by Charles Babbage*, translated and annotated by Ada Lovelace. London: Richard & John E. Taylor.

[2] A.Haché (26 June 2023). *Feminist Infrastructure: The Creation of What Sustains Us.* GenderIT. Accessed 25 April 2025. https://genderit.org/feminist-talk/feminist-infrastructure-creation-what-sustains-us

[3] S. Cupler. (26 May 2023). *A brief overview of AI use in WANA*. SMEX. Accessed 24 March 2025. https://smex.org/a-brief-overview-of-ai-use-in-wana

[4] The interview with Shared Planet was conducted with three people.

[5] Association for Progressive Communications. (2024). *Feminist Principles of the Internet – Version 2.0*. Accessed 24 March 2025. https://www.apc.org/en/pubs/feminist-principles-internet-version-20

[6] J. Guerra. (2022). *Towards a Feminist Framework for AI Development: From Principles to Practice*. Feminist AI. Accessed 24 March 2025. https://feminis-tai.pubpub.org/pub/ghxn5ka8/release/2

[7] Mozilla. (n.d.). *Trustworthy Artificial Intelligence*. Accessed 24 March 2025. https://foundation.mozilla.org/en/internet-health/trustworthy-artificial-intelligence

[8] H. Kunzru. (1997). *The unlikely cyborg*. *Wired UK*, 2(12). Accessed 24 March 2025. https://archive.gyford.com/1997/wired-uk/2.12/features/haraway.html

[9] J. Radloff (6 June 2017). *The internet of memory: First we'll take Huairou and then we'll take New York. Hacking the UN to code technology and women's rights into the system.* Accessed 25 April 2025. https://www.apc.org/en/blog/internet-memory-first-well-take-huairou-and-then-well-take-new-york-hacking-un-code-technology

[10] GenderIT.org. (2024). *Feminist Principles of the Internet*. Accessed 10 February 2025. https://www.genderit.org/articles/feminist-principles-internet

[11] Mozilla. (n.d.). *Trustworthy Artificial Intelligence*, op. cit.

[12] M.O. Jones. (2022). *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. London: Hurst.

[13] Tahrir Institute for Middle East Policy. (2019). *TIMEP Brief: Export of Surveillance to MENA Countries*. Accessed 24 March 2025. https://timep.org/2019/10/23/timep-brief-export-of-surveillance-to-mena-countries

[14] S. Cupler. (11 November 2024). Interview with author.

[15] A. Abrougui. (2025). 'Phishing, Spyware, and Smart City Tech: Surveillance in Sisi's Egypt'. In *Digital Surveillance in Africa: Power, Agency, and Rights*, edited by T. Roberts and A. Mare, 57–84. London: Zed Books. Accessed 14 February 2025. http://dx.doi.org/10.5040/9781350422117.ch-3

[16] Ž. Švedkauskas. (2022). *Digital Surveillance, Master Key for MENA Autocrats*. EuroMeSCo. Accessed 24 March 2025. https://www.euromesco.net/wp-content/uploads/2022/07/Policy-Study27.pdf

[17] Ž. Švedkauskas (2022). *Digital Surveillance*, op. cit.

[18] J. Dalek, L. Gill, B. Marczak, S. McKune, N. Noor, J. Oliver, J. Penney, A. Senft and R. Deibert. (2018). *Planet Netsweeper*. Citizen Lab. Accessed 24 March 2025. https://citizenlab.ca/2018/04/planet-netsweeper

[19] Ibid.

[20] International Federation for Human Rights. (26 July 2021). *The Pegasus Project: sale of surveillance technology to autocratic governments must stop*. Accessed 24 March 2025.

https://www.fidh.org/en/region/north-africa-middle-east/the-pegasus-project-sale-of-surveillance-technology-to-autocratic

[21] J. Warminsky. (7 September 2023). *Apple discloses zero-days linked to NSO Group spyware*. The Record. Accessed 24 March 2025. https://therecord.media/apple-discloses-two-zero-days-in-new-updates

[22] Ž. Švedkauskas. (2022). *Digital Surveillance*, op. cit.

[23] A. D'Andrea. (13 September 2024). *How AI is making phishing attacks more dangerous*. Keeper Security blog. Accessed 24 March 2025. https://www.keepersecurity.com/blog/2024/09/13/how-ai-is-making-phishing-attacks-more-dangerous/

[24] Ibid.

[25] Ibid.

[26] M. Fatafta and D. Samaro. (2021). *Exposed and Exploited: Data Protection in the Middle East and North Africa*. Access Now. Accessed 24 March 2025. https://www.accessnow.org/wp-content/uploads/2021/01/Access-Now-MENA-data-protection-report.pdf

[27] M. Fatafta. (4 December 2024). Interview with author.

[28] Amnesty International. (2 May 2023). *Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid*. Accessed 24 March 2025. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] S. Cupler. (2023). *A brief overview of AI use*, op. cit.

[33] K. Zidan. (8 December 2022). *The Qatar World Cup ushers in a new era of digital authoritarianism in sports.* The Nation. Accessed 24 March 2025. https://www.thenation.com/article/society/qatar-world-cup-surveillance

[34] S. Cupler. (2023). *A brief overview of AI use*, op. cit.

[35] A. Dawood. (24 November 2021). *AI looks at historical data to predict future crimes for UAE's police force*. Mashable Middle East. Accessed 24 March 2025. https://me.mashable.com/tech/15800/ai-looks-at-historical-data-to-predict-future-crimes-for-uaes-police-force

[36] H. Alakaleek. (2023). *Facial recognition technology usage in Jordan*. Jordan News. Accessed 24 March 2025. https://www.jordannews.jo/Section-36/Opinion/Facial-recognition-technology-usage-in-Jordan-31219

[37] F. Belaïd, R. Amine and C. Massie. (2024). 'Smart Cities Initiatives and Perspectives in the MENA Region and Saudi Arabia'. In *Smart Cities. Studies in*

Energy, Resource and Environmental Economics, edited by F. Belaïd and A. Arora. Cham: Springer. Accessed 24 March 2025. https://doi.org/10.1007/978-3-031-35664-3_16

[38] Thomson Reuters Foundation. (4 January 2023). *FEATURE-CCTV cameras will watch over Egyptians in new high-tech capital*. Reuters. Accessed 24 March 2025. https://www.reuters.com/article/business/media-telecom/feature-cctv-cameras-will-watch-over-egyptians-in-new-high-tech-capital-idUSL8N33I0DO

[39] Š. Waisová. (2022). 'The Tragedy of Smart Cities in Egypt: How the Smart City is Used towards Political and Social Ordering and Exclusion'. *Applied Cybersecurity & Internet Governance*, 1(1), 1–10. Accessed 24 March 2025. https://www.acigjournal.com/pdf-184286-105044?filename=The%20Tragedy%20of%20Smart.pdf

[40] A. Abrougui. (2025). 'Phishing, Spyware', op. cit.

[41] M. Fatafta. (4 December 2024). Interview with author.

[42] L. Derfner (16 September 2024). *Against spy revelations, Israel doth protest too much.* +972 Magazine. Accessed 31 July 2025. https://www.972mag.com/against-spy-revelations-israel-doth-protest-too-much/

[43] M. Fatafta and Front Line Defenders. (8 May 2023). *Unsafe anywhere: women human rights defenders speak out about Pegasus attacks*. Access Now. Accessed 24 March 2025. https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan

[44] Doxxing is the practice of disseminating personal information of someone with the purpose of intimidating and harassing them. This information can be gathered using publicly available sources such as social media posts or through unauthorized access such as hacking or digital surveillance tactics.

[45] M. Fatafta and D. Samaro. (2021). *Exposed and Exploited*, op. cit.

[46] Privacy International. (22 July 2022). *Privacy and sexual and reproductive health in a post-Roe world*. Accessed 10 February 2025. https://privacyinternational.org/long-read/4937/privacy-and-sexual-and-reproductive-health-post-roe-world

[47] R. George. (7 December 2023). *The AI assault on women: what Iran's tech enabled morality laws indicate for women's rights movements*. Council on Foreign Relations blog. Accessed 24 March 2025. https://www.cfr.org/blog/ai-assault-women-what-irans-tech-enabled-morality-laws-indicate-womens-rights-movements

[48] Human Rights Watch. (2023). *Trapped: How Male Guardianship Policies Restrict Women's Travel and Mobility in the Middle East and North Africa*. Accessed 24 March 2025. https://www.hrw.org/report/2023/07/18/trapped/how-male-guardianship-policies-restrict-womens-travel-and-mobility-middle

[49] Ibid.

[50] M. Browne and N. Casey. (18 July 2024). *Spain's domestic violence algorithm: can AI prevent abuse or does it fail victims? The New York Times*. Accessed 24 March 2025. https://www.nytimes.com/interactive/2024/07/18/technology/spain-domestic-violence-viogen-algorithm.html [paywall]

[51] A. Satariano and R. Toll Pifarré (17 January 2025). *Spain Overhauls Domestic Violence System After Criticism.* The New York Times. Accessed 30 July 2025.

https://www.nytimes.com/2025/01/17/technology/spain-domestic-violence-algorithm.html

[52] J. Kelley. (17 December 2020). *A decade after the Arab Spring, platforms have turned their backs on critical voices in the Middle East and North Africa*. Electronic Frontier Foundation. Accessed 24 March 2025.

https://www.eff.org/deeplinks/2020/12/decade-after-arab-spring-platforms-have-turned-their-backs-critical-voices-middle

[53] R. Gorwa, R. Binns and C. Katzenbach. (2020). *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*. Big Data & Society, 7(1). Accessed 28 April 2025. https://doi.org/10.1177/2053951719897945

[54] Meta. (18 October 2023). *How technology detects violations.* Accessed 28 April 2025, https://transparency.meta.com/en-gb/enforcement/detecting-violations/technology-detects-violations/

[55] SMEX. (2024). *From Sharing to Silence: Assessing Social Media Suppression of SRHR Content in WANA*. Accessed 24 March 2025. https://smex.org/from-sharing-to-silence-assessing-social-media-suppression-of-srhr-content-in-wana

[56] M. Elswah. (2024). *Does AI understand Arabic? Evaluating the Politics Behind the Algorithmic Arabic Content Moderation.* Carr Center for Human Rights Policy. Issue 2024-01. Accessed 28 April 2015.

[57] Business for Social Responsibility (BSR). (2022). *Human Rights Due Diligence of Meta's Impacts in Israel and Palestine in May 2021: Insights and Recommendations*. Accessed 24 March 2025. https://www.bsr.org/reports/BSR_Meta_Human_Rights_Israel_Palestine_English.pdf

[58] Ibid.

[59] Meta. (2024). *Meta Update: Israel and Palestine Human Rights Due Diligence*. Accessed 24 March 2025. https://humanrights.fb.com/wp-content/uploads/2024/09/Israel-Palestine-HRDD-Implementation-update-2024.pdf

[60] Human Rights Watch. (2023). *Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook*. Accessed 24 March 2025. https://www.hrw.org/sites/default/files/media_2023/12/ip_meta1223%20web.pdf

[61] Office of the High Commissioner for Human Rights (OHCHR). (18 March 2025). *Israel ramps up settlement and annexation in West Bank with dire human rights consequences*. Press release. Accessed 24 March 2025. https://www.ohchr.org/en/press-releases/2025/03/israel-ramps-settlement-and-annexation-west-bank-dire-human-rights

[62] Human Rights Watch. (2023). *Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook*. Accessed 24 March 2025. https://www.hrw.org/sites/default/files/media_2023/12/ip_meta1223%20web.pdf

[63] Meta. (13 October 2023). *Meta's ongoing efforts regarding the Israel-Hamas war.* Accessed 24 March 2025. https://about.fb.com/news/2023/10/metas-efforts-regarding-israel-hamas-war

[64] Human Rights Watch. (2023). *Meta's Broken Promises*, op. cit.

[65] Committee to Protect Journalists. (4 February 2025). *Journalist Casualties in the Israel-Gaza War*. Accessed 24 March 2025. https://cpj.org/2024/12/journalist-casualties-in-the-israel-gaza-conflict

[66] M. Fatafta, A. Sibai, Z. Rosson, K. Mneja, H. Kreitem and S. Cheng. (10 November 2023). *Palestine unplugged: how Israel disrupts Gaza's internet*. Accessed 24 March 2025.

https://www.accessnow.org/publication/palestine-unplugged

[67] D. Kayyali and R. Althaibani. (2017). *Vital human rights evidence in Syria is disappearing from YouTube*. Witness blog. Accessed 24 March 2025. https://blog.witness.org/2017/08/vital-human-rights-evidence-syria-disappearing-youtube

[68] W. Eskandar. (23 October 2019). *How Twitter is gagging Arabic users and acting as morality police*. openDemocracy. Accessed 24 March 2025. https://www.opendemocracy.net/en/north-africa-west-asia/how-twitter-gagging-arabic-users-and-acting-morality-police

[69] SMEX. (2024). *From Sharing to Silence: Assessing Social Media Suppression of SRHR Content in WANA*. Accessed 24 March 2025. https://smex.org/from-sharing-to-silence-assessing-social-media-suppression-of-srhr-content-in-wana

[70] Ibid.

[71] D. Oraby. (2024) 'Sexuality Education for Youth and Adolescents in the Middle East and North Africa Region: A Window of Opportunity'. *Global Health, Science and Practice*, 12(1), e2300282.

[72] 7amleh. (2023). *An Analysis of the Israeli Inciteful speech against the Village of 'Huwara' on Twitter*. Accessed 24 March 2025. https://7amleh.org/2023/06/01/7amleh-issues-an-analysis-of-the-israeli-inciteful-speech-against-the-village-of-huwara-on-twitter

[73] BSR. (2022). *Human Rights Due Diligence*, op. cit.

[74] OHCHR. (4 November 2023). *UN human rights chief condemns rise in hatred*. Accessed 24 March 2025. https://www.ohchr.org/en/press-releases/2023/11/un-human-rights-chief-condemns-rise-hatred

[75] J. Salhani. (28 August 2024). Targeted: *how misinformation puts Lebanon's Syrian refugees in danger*. Tahrir Institute for Middle East Policy. Accessed 24 March 2025.

https://timep.org/2024/08/28/targeted-how-misinformation-puts-lebanons-syrian-refugees-in-danger

[76] A. Abrougui and R. Asad. (2021). *Digital Safety is a Right: Syrian Women Journalists and Human Rights Defenders in the Digital Space: Risks and Threats*. Syrian Female Journalists Network. Accessed 24 March 2025. https://media.sfjn.org/en/digital-safety-is-a-right

[77] A. Leber and A. Abrahams. (2021). *Social Media Manipulation in the MENA: Inauthenticity, Inequality, and Insecurity*. Project on Middle East Political Science. Accessed 24 March 2025. https://pomeps.org/social-media-manipulation-in-the-mena-inauthenticity-inequality-and-insecurity

[78] A group of individuals acting in coordination online and on behalf of an entity such as a government or political party to spread propaganda and/or attack critics.

[79] K. Benner, M. Mazzetti, B. Hubbard and M. Isaac. (20 October 2018). *Saudis' image makers: a troll army and a Twitter insider*. *The New York Times*. Accessed 24 March 2025.

https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html [paywall]

[80] D. Klepper. (28 November 2023). *Fake babies, real horror: deepfakes from the Gaza war increase fears about AI's power to mislead*. The Associated Press. Accessed 24 March 2025. https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47

[81] D. Milmo. (8 February 2024). *Iran-backed hackers interrupt UAE TV streaming services with deepfake news*. The *Guardian*. Accessed 24 March 2025.

https://www.theguardian.com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news

[82] K. Wagner. (9 July 2024). *The awful plan to turn Gaza into the next Dubai*. The Nation. Accessed 24 March 2025. https://www.thenation.com/article/world/gaza-2035-aec-neom-saudi

[83] A. Kawash. (8 November 2024). Interview with author.

[84] Gulf Centre for Human Rights. (14 October 2019). *Deepfake poses a threat to human rights defenders in the Middle East*. Accessed 24 March 2025. https://www.gc4hr.org/deepfake-poses-a-threat-to-human-rights-defenders-in-the-middle-east

[85] A. Al-Kaisy. (2022). *Online Violence Towards Women in Iraq*. Elbarlament. Accessed 24 March 2025. https://elbarlament.org/wp-content/uploads/2022/03/Aida-2.pdf

[86] O. Ibrahim. (21 November 2024). Interview with author.

[87] M. Elswah. (24 October 2024). Interview with author.

[88] K. Blouin and G. Daswani. (2023). *Orientalism through Time and Place: A Virtual Exhibit*. Everyday Orientalism. Accessed 24 March 2025. https://everydayorientalism.wordpress.com/2023/08/11/orientalism-through-time-and-place-a-virtual-exhibit

[89] M. Elswah. (24 October 2024). Interview with author.

[90] M. Alimardani and M. Elswah. (2021). *Digital Orientalism: #SaveSheikhJarrah and Arabic Content Moderation*. Project on Middle East Political Science. Accessed 24 March 2025.

https://pomeps.org/digital-orientalism-savesheikhjarrah-and-arabic-content-moderation

[91] Meta. (n.d.) *Policy: Dangerous Organizations and Individuals*. Accessed 7 March 2024.

https://transparency.fb.com/en-gb/policies/community-standards/dangerous-individuals-organizations

[92] S. Biddle. (2021). *Revealed: Facebook's secret blacklist of 'dangerous individuals and organizations'*. The Intercept. Accessed 24 March 2025. https://theintercept.com/2021/10/12/facebook-secret-blacklist-dangerous

[93] Ibid.

[94] BSR. (2022). *Human Rights Due Diligence*, op. cit.

[95] M. Jarrar. (27 November 2024). Interview with author.

[96] Ibid.

[97] M. Elswah. (24 October 2024). Interview with author.

[98] G. Nicholas and A. Bhatia. (23 May 2023). *The dire defect of 'multilingual' AI content moderation*. Wired. Accessed 24 March 2025. https://www.wired.com/story/content-moderation-language-artificial-intelligence

[99] G. Nicholas and A. Bhatia. (2023). *Lost in Translation: Large Language Models in Non-English Content Analysis*. Center for Democracy & Technology. Accessed 24 March 2025. https://cdt.org/wp-content/uploads/2023/05/non-en-content-analysis-primer-051223-1203.pdf

[100] Ibid.

[101] M. Elswah. (24 October 2024). Interview with author.

[102] A. El Masri. 22 October 2024). Interview with author.

[103] A. Abrougui. (17 May 2021). *Hate speech: why social media platforms are failing the LGBTQ community*. Jeem. Accessed 24 March 2025. https://jeem.me/en/internet/548

[104] Z. Shoshana. (2019). *The Age of Surveillance Capitalism*. New York: Public Affairs.

[105] CompaniesMarketCap. (2025). *Largest Companies by Market Cap*. Accessed 24 March 2025. https://companiesmarketcap.com

[106] A. Khan, E. Tant and C. Harper. (2023). *Facing the backlash: what is fueling anti-feminist and anti-democratic forces.* ALIGN. Accessed 29 April 2025. https://www.alignplatform.org/sites/default/files/2023-07/align-framingpaper-backlash-web.pdf

[107] The manosphere is "a collection of websites, social media accounts and forums dedicated to men's issues" many of which "have become spaces where explicit anti-women and anti-feminist sentiment abound. See: R. Lawson (2023). *A dictionary of the manosphere: five terms to understand the language of online male supremacists".* The Conversation. Accessed 29 April 2025. https://theconversation.com/a-dictionary-of-the-manosphere-five-terms-to-understand-the-language-of-online-male-supremacists-200206

[108] S. Kaddoura (2024). *The Arab Manosphere: a New Wave of Western Misogyny in the MENA Region*. Friedrich-Ebert-Stiftung. Accessed 29 April 2025. https://feminism-mena.fes.de/e/the-arab-manosphere-a-new-wave-of-western-misogyny-in-the-mena-region.html.

[109] R. Hall. (2025). *Beyond Andrew Tate: the imitators who help promote misogyny online.* The Guardian. Accessed 29 April 2025. https://www.theguardian.com/media/2025/mar/19/beyond-andrew-tate-the-imitators-who-help-promote-misogyny-online

[110] A digital marketing system where content creators or influencers are hired by businesses to promote their products and services, and even destinations and events, in exchange for money or other perks.

[111] S. Bishop. (2021). 'Influencer Management Tools: Algorithmic Cultures, Brand Safety, and Bias'. *Social Media + Society*, 7(1). Accessed 24 March 2025. https://doi.org/10.1177/20563051211003066

[112] R. Hall. (2025). *Beyond Andrew Tate: the imitators who help promote misogyny online.* The Guardian. Accessed 29 April 2025.

https://www.theguardian.com/media/2025/mar/19/beyond-andrew-tate-the-imitators-who-help-promote-misogyny-online

[113] N. Naim. (23 October 2024). Interview with author.

[114] A. Kentikelenis, S. Mechmech, A. Bouzaiene, R. Moshrif and N. Abdo. (2023). *The Middle East and North Africa Gap: Prosperity for the Rich, Austerity for the Rest*. Oxfam International. Accessed 24 March 2025. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621549/bp-mena-gap-prosperity-for-the-rich-austerity-for-the-rest-051023-en.pdf;jsessionid=BA190CBC6CD421DA5A0272E239CAB69F?sequence=13

[115] Ibid.

[116] International Labour Organization. (2025). *Unemployment, Total (% of Total Labor Force) (Modeled ILO Estimate) – Middle East & North Africa*. World Bank Group. Accessed 24 March 2025. https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?locations=ZQ&name_desc=false

[117] International Labor Organization. (2024). *Global Employment Trends for Youth 2024: Middle East and North Africa*. Accessed 24 March 2025. https://www.ilo.org/sites/default/files/2024-08/MENA%20GET%20Youth%20Brief%202024.pdf

[118] World Bank. (2025). *World Development Indicators Database: Labor Force, Female (% of Total Labor Force) – Middle East & North Africa*. Accessed 14 February 2025. https://data.worldbank.org/indicator/SL.TLF.TOTL.FE.ZS?end=2023&locations=ZQ&start=1990&view=chart

[119] World Economic Forum. (2017). *The Future of Jobs and Skills in the Middle East and North Africa*. Accessed 24 March 2025. https://www3.weforum.org/docs/WEF_EGW_FOJ_MENA.pdf

[120] S. Cupler. (2023). *A brief overview of AI use*, op. cit.

[121] N. Lewis and R. Bendimerad. (16 September 2024). *Why these Gulf states want to be AI superpowers.* CNN. Accessed 24 April 2025. https://edition.cnn.com/2024/09/16/middleeast/middle-east-artificial-intelligence-spc/index.html

[122] N. Rizk. (2020). 'Artificial Intelligence and Inequality in the Middle East: The Political Economy of Inclusion'. In *The Oxford Handbook of Ethics of AI*, edited by M.D. Dubber, F. Pasquale and S. Das, 625–49. Oxford: Oxford University Press.

[123] N. Rizk. (31 October 2024). Interview with author.

[124] A. Hashem. (2024). *Connectivity in the Middle East and North Africa: A Fact-Finding Study*. Internet Society. Accessed 24 March 2025. https://www.internetsociety.org/wp-content/uploads/2024/06/MENA-Connectivity-Report-EN.pdf

[125] A. Eck. (2024). *Mapping Tech Companies' Cloud Expansion in the Gulf and its Human Rights Implications*. SMEX. Accessed 24 March 2025. https://smex.org/wp-content/uploads/2024/03/Mapping-report-Final.pdf

[126] A. Kawash. (8 November 2024). Interview with author.

[127] S. Scheer. (29 May 2023). *Nvidia to build Israeli supercomputer as AI demand soars*. Reuters. Accessed 24 March 2025. https://www.reuters.com/technology/nvidia-build-israeli-supercomputer-ai-demand-soars-2023-05-29

[128] N. Rizk. (2020) 'Artificial Intelligence', op. cit.

[129] B. Perrigo. (20 March 2024). *The UAE is on a mission to become an AI power.* Time.

Accessed 24 March 2025. https://time.com/6958369/artificial-intelligence-united-arab-emirates

[130] Ibid.

[131] A. El Masri. (22 October 2024). Interview with author.

[132] N. Rizk. (2020). 'Artificial Intelligence', op. cit.

[133] N. Rizk. (21 October 2024). Interview with author.

[134] World Economic Forum. (2017). *The Future of Jobs and Skills*, op. cit.

[135] Ibid.

[136] International Labor Organization. (2019). *State of Skills: Tunisia*. Accessed 14 February 2025. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_emp/%40emp_ent/documents/genericdocument/wcms_736691.pdf

[137] N. Rizk. (2020). 'Artificial Intelligence', op. cit.

[138] M. Chui, J. Manyika and M. Miremadi. (12 April 2017). *The countries most (and least) likely to be affected by automation*. Harvard Business Review. Accessed 24 March 2025. https://hbr.org/2017/04/the-countries-most-and-least-likely-to-be-affected-by-automation

[139] P. Gmyrek, J. Berg and D. Bescond. (2023). *Generative AI and Jobs: A Global Analysis of Potential Effects on Job Quantity and Quality*. ILO Working Paper 96. International Labour Organization. Accessed 24 March 2025. https://researchrepository.ilo.org/esploro/outputs/encyclopediaEntry/995326516102676

[140] S. Ahmed. (8 September 2024). *Le télémarketing: Un secteur négligé malgré ses contributions cruciales à l'économie tunisienne*. LaPresse. [French]. Accessed 24 March 2025.

https://lapresse.tn/2024/09/08/le-telemarketing-un-secteur-neglige-malgre-ses-contributions-cruciales-a-leconomie-tunisienne

[141] Hamza M. (8 April 2024). *Intelligence Artificielle, le grand remplacement dans les centres d'appels marocains?* TRT Français. [French]. Accessed 24 March 2025.

https://www.trtfrancais.com/actualites/intelligence-artificielle-le-grand-remplacement-dans-les-centres-dappels-marocains-17699021

[142] P. Gmyrek, J. Berg and D. Bescond. (2023). *Generative AI and Jobs: A Global Analysis of Potential Effects on Job Quantity and Quality*. ILO Working Paper 96. International Labour Organization. Accessed 24 March 2025. https://researchrepository.ilo.org/esploro/outputs/encyclopediaEntry/995326516102676

[143] F. Khafagy, Z.A. Khalik and O. Naji. (2021). *Women's Economic Justice and Rights in the Arab Region*. Arab State Civil Society Organizations and Feminists Networks. Accessed 24 March 2025. https://arabstates.unwomen.org/sites/default/files/Field%20Office%20Arab%20States/Attachments/2021/07/Womens%20Economic%20Justice%20and%20Rights-Policy%20Paper-EN.pdf

[144] H. Nazier. (2019). *Women's Economic Empowerment: An Overview for the MENA Region*. European Institute of the Mediterranean. Accessed 24 March

2025. https://www.iemed.org/publication/womens-economic-empowerment-an-overview-for-the-mena-region

[145] Abbott, P. (2017). *Gender Equality and MENA Women's Empowerment in the Aftermath of the 2011 Uprisings*. Arab Transformations Working Paper n. 10. Aberdeen: University of Aberdeen. Accessed 25 April 2025.

[146] Global Campus on Human Rights. (2024). *Gender digital divide: the new face of inequality in the MENA region*. Accessed 24 March 2025. https://gchuman-rights.org/gc-preparedness/preparedness-gender/article-detail/gender-digi-tal-divide-the-new-face-of-inequality-in-the-mena-region.html

[147] N. Rizk. (2020). 'Artificial Intelligence', op. cit.

[148] C. Collett, G. Neff and L. Gouvea Gomes. (2022). *The Effects of AI on the Working Lives of Women*. UNESCO, OECD and the Inter-American Development Bank. Accessed 24 March 2025. https://www.oecd.org/con-tent/dam/oecd/en/publications/reports/2022/03/the-effects-of-ai-on-the-working-lives-of-women_1b627535/14e9b92c-en.pdf

[149] Maharat. https://maharat.ma. Accessed 14 February 2025.

[150] Look Up Tunisie. (n.d.). *Les Nouvelles Technologies dans le Recrutement*. [French]. Accessed 14 February 2025. https://www.lookuptunisie.com/les-nouvelles-technologies-dans-le-recrutement

[151] Arabian Business. (15 October 2024). *UAE jobs: AI-powered recruitment surges 90 per cent as tech firms look to hire top talent*. Accessed 24 March 2025. https://www.arabianbusiness.com/jobs/uae-jobs-ai-powered-recruit-ment-surges-90-per-cent-as-tech-firms-look-to-hire-top-talent

[152] Kader. (n.d.). *Get to Know Kader*. Accessed 14 February 2025. https://www.kaderapp.com/en/about-us

[153] Z. Chen. (2023). 'Ethics and Discrimination in Artificial Intelligence-Enabled Recruitment Practices'. *Humanities and Social Sciences Communications*, 10, 567. Accessed 24 March 2025. https://doi.org/10.1057/s41599-023-02079-x

[154] S. Cupler. (11 November 2024). Interview with author.

[155] N. Naim. (23 October 2024). Interview with author.

[156] N. Kahil. (n.d.). *The Women in MENA Tech Survey*. Wired Middle East. Accessed 24 March 2025. https://wired.me/culture/the-women-in-mena-tech-survey

[157] LinkedIn. (n.d.). *AI-Powered Features*. Accessed 14 February 2025. https://training.talent.linkedin.com/page/ai-powered-features#language_english

[158] Bayt. (n.d.). *Hire 2x Faster with Bayt AI+ Hiring Tool*. Accessed 10 December 2024. https://www.bayt.com/en/employers/bayt-aiplus-hiring-tool

[159] N. Rizk. (2020). 'Artificial Intelligence', op. cit.

[160] Z. Siddiqui and Y. Zhou. (21 September 2021). *How the platform economy sets women up to fail*. Rest of World. Accessed 24 March 2025. https://restofworld.org/2021/global-gig-workers-how-platforms-set-women-up-to-fail

[161] B. Athreya. (2021). *Bias In, Bias Out: Gender and Work in the Platform Economy*. International Development Research Centre. Accessed 24 March 2025.

https://idl-bnc-idrc.dspacedirect.org/items/7d8e2f97-b1dd-49ad-9843-a0480f5f80eb

[162] Fairwork. (2022). *Domestic Platform Work in the Middle East and North Africa*. Accessed 24 March 2025. https://fair.work/wp-content/uploads/sites/17/2022/12/Fairwork-MENA-report-2022-en.pdf

[163] N. Rizk, N. Salem and N. Weheba. (2018). 'A Gendered Analysis of Ridesharing: Perspectives from Cairo, Egypt'. In *Urban Transport in the Sharing Economy Era*. Center for the Implementation of Public Policies for Equity and Growth (CIPPEC). Accessed 24 March 2025. https://www.cippec.org/wp-content/uploads/2018/09/UrbanTransport-completo-web_CIPPEC.pdf

[164] Ibid.

[165] B. Athreya. (2021). *Bias In, Bias Out*, op. cit.

[166] Ibid.

[167] N. Rizk. (31 October 2024). Interview with author.

[168] Ibid.

[169] N. Rizk. (21 October 2024). Interview with author.

[170] United Nations Office for Disarmament Affairs. (n.d.). *Lethal Autonomous Weapon Systems (LAWS)*. Accessed 24 March 2025. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw

[171] Ibid.

[172] United Nations Human Rights Council. (2013). *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, A/HRC/23/47 (9 April 2013).* Accessed 24 March 2025. https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf

[173] Y. Serhan. (18 December 2024). *How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare.* Time Magazine. Accessed 25 April 2025. https://time.com/7202584/gaza-ukraine-ai-warfare/

[174] S. Frenkel and N. Odenheimer (25 April 2025). *Israel's A.I. Experiments in Gaza War Raise Ethical Concerns.* New York Times. Accessed 25 April 2025. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html

[175] https://www.asil.org/insights/volume/29/issue/1

[176] N. Naim. (23 October 2024). Interview with author.

[177] International Committee of the Red Cross (ICRC). (n.d.). *Fundamental Principles of IHL*. Accessed 24 March 2025. https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl

[178] A. Kawash. (8 November 2024). Interview with author.

[179] B. McKernan and H. Davies. (3 April 2024). *Israel announces expanded use of AI database to track Hamas and airstrikes in Gaza*. The *Guardian*. Accessed 24 March 2025. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

[180] Y. Abraham. (3 April 2024). *Lavender AI: inside the Israeli Army's AI capabilities in Gaza*. 972 Magazine. Accessed 24 March 2025. https://www.972mag.com/lavender-ai-israeli-army-gaza

[181] Israel's Use of AI in Gaza May Be Setting a New Warfare Norm | TIME

[182] Amnesty International. (2023). *Israel/OPT*, op. cit.

[183] M. Griffiths and J. Repo. (2021). 'Women and Checkpoints in Palestine'. *Security Dialogue*, 52(3), 249–65. Accessed 25 March 2025. https://doi.org/10.1177/0967010620918529

[184] Ibid.

[185] Y. Abraham. (2024). *Lavender AI*, op. cit.

[186] Ibid.

[187] OHCHR. (15 April 2024). Gaza: UN experts deplore use of purported AI to commit 'domicide' in Gaza, call for reparative approach to rebuilding. Press release. Accessed 24 March 2025. https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call

[188] S. Cupler. (11 November 2024). Interview with author.

[189] United Nations Office for the Coordination of Humanitarian Affairs (OCHA). (20 November 2023). *Hostilities in the Gaza Strip and Israel: reported impact, day 45*. Accessed 24 March 2025. https://www.ochaopt.org/content/hostilities-gaza-strip-and-israel-reported-impact-day-45

[190] Human Rights Watch. (15 November 2023). *Gaza communications blackout imminent due to fuel shortage*. Accessed 24 March 2025. https://www.hrw.org/news/2023/11/15/gaza-communications-blackout-imminent-due-fuel-shortage

[191] H. Al-Shalchi. (3 March 2024). *Destruction from the war with Israel has cut Gaza off from the outside world.* NPR. Accessed 24 March 2025. https://www.npr.org/2024/03/03/1229402063/gaza-communications-cell-phone-internet-service-blackouts-paltel

[192] *The New York Times*. (16 October 2023). *Gaza invasion: Israel accessing cellphone data*. Accessed 24 March 2025. https://www.nytimes.com/2023/10/16/world/middleeast/gaza-invasion-israel-cellphone-data.html [paywall]

[193] Human Rights Watch. (10 September 2024). *Questions and answers on the Israeli military's use of digital tools in Gaza*. Accessed 24 March 2025. https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza

[194] E. Farge (8 November 2024). *Gaza women, children are nearly 70% of verified war dead, UN rights office says*. Reuters. Accessed 24 March 2025. https://www.reuters.com/world/middle-east/nearly-70-gaza-war-dead-women-children-un-rights-office-says-2024-11-08

[195] Oxfam International. (30 September 2024). *More women and children killed in Gaza by Israeli military than any other recent conflict in a single year – Oxfam*. Press release. Accessed 24 March 2025. https://www.oxfam.org/en/press-releases/more-women-and-children-killed-gaza-israeli-military-any-other-recent-conflict

[196] Ibid.

[197] Ibid.

[198] OHCHR. (13 March 2025). *'More than a human can bear': Israel's systematic use of sexual, reproductive and other forms of gender-based violence since October 2023*. Press release. Accessed 24 March 2025.

https://www.ohchr.org/en/press-releases/2025/03/more-human-can-bear-israels-systematic-use-sexual-reproductive-and-other

[199] Abdul Samad, Lama; Butcher, Martin; Khalidi, Bushra, (18 July 2024), Water War Crimes: How Israel has weaponised water in its military campaign in Gaza. Accessed 17 July 2025. https://policy-practice.oxfam.org/resources/water-war-crimes-how-israel-has-weaponised-water-in-its-military-campaign-in-ga-621609/

[200] D. Pittis. (4 May 2023). *Canadian artificial intelligence leader Geoffrey Hinton piles on fears of computer takeover.* CBC News. Accessed 25 April 2025. https://ici.radio-canada.ca/rci/en/news/1976822/canadian-artificial-intelligence-leader-geoffrey-hinton-piles-on-fears-of-computer-takeover

[201] A. Loewenstein. (2023). *The Palestine Laboratory: How Israel Exports the Technology of Occupation around the World*. London: Verso Books.

[202] Ibid.

[203] Amnesty International. (2015). *Autonomous Weapons Systems: Five Key Human Rights Issues for Consideration*. Accessed 24 March 2025. https://www.amnesty.org/en/wp-content/uploads/2023/05/ACT3014012015ENGLISH.pdf

[204] ICRC. (9 December 2024). *ICRC: 'We have the chance to improve the lives of millions'*. Press release. Accessed 24 March 2025. https://www.icrc.org/en/unga79-50th-session-humanitarian-relief-assistance

[205] M. Suliman. (23 October 2024). *The deepfake is a powerful weapon in the war in Sudan*. African Arguments. Accessed 24 March 2025. https://africanarguments.org/2024/10/the-deepfake-is-a-powerful-weapon-in-the-war-in-sudan

[206] J. Goodman and M. Hashim. (5 October 2023). *AI: voice cloning tech emerges in Sudan civil war.* BBC News. Accessed 24 March 2025. https://www.bbc.com/news/world-africa-66987869

[207] A. Davies and BBC Arabic. (30 May 2024). *All eyes on Rafah: the post that's been shared by more than 47m people*. BBC News. Accessed 24 March 2025. https://www.bbc.com/news/articles/cjkkj5jejleo

[208] 7amleh. (2024). *Fine-tuning Large Language Models for the Larger World*. YouTube. Accessed 24 March 2025. https://www.youtube.com/watch?v=1SzKHqVfuoE

[209] D. Saber. (24 October 2024). Interview with author.

[210] Ibid.

[211] J. Bhuiyan. (2023). *WhatsApp's AI shows gun-wielding children when prompted with 'Palestine'*. The *Guardian*. Accessed 24 March 2025. https://www.theguardian.com/technology/2023/nov/02/whatsapps-ai-palestine-kids-gun-gaza-bias-israel

[212] A. Kawash. (2023). *What a cat in a keffiyeh reveals about AI's anti-Palestinian bias*. +972 Magazine. Accessed 24 March 2025. https://www.972mag.com/ai-bias-palestinian-cat-keffiyeh

[213] A. Kawash. (8 November 2024). Interview with author.

[214] Ibid.

[215] Al Jazeera. (23 April 2024). *What is Project Nimbus, and why are Google workers protesting Israel deal?* Accessed 10 February 2025. https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal

[216] Ibid.

[217] C. Haskins. (15 July 2024). *Amazon and Google workers speak out against 'Project Nimbus' to supply Israel's IDF*. Wired. Accessed 24 March 2025. https://www.wired.com/story/amazon-google-project-nimbus-israel-idf [pay-wall]

[218] S. Biddle. (2 December 2024). *Documents contradict Google's claims about its Project Nimbus contract with Israel*. The Intercept. Accessed 24 March 2025. https://theintercept.com/2024/12/02/google-project-nimbus-ai-israel

[219] M. Jarrar. (27 November 2024). Interview with author.

[220] No Tech For Apartheid. http://www.notechforapartheid.com. Accessed 24 March 2025.

[221] A. Kawash. (8 November 2024). Interview with author.

[222] F. Albanese. (30 June 2025) *From economy of occupation to economy of genocide.* Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. UN Human Rights Council. Accessed 17 July 2025. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

[223] M. Mahmoud. (19 April 2024). *The Looming Climate and Water Crisis in the Middle East and North Africa*. Carnegie Endowment for International Peace. Accessed 24 March 2025. https://carnegieendowment.org/research/2024/04/the-looming-climate-and-water-crisis-in-the-middle-east-and-north-africa?lang=en

[224] United Nations High Commissioner for Refugees (UNHCR). *Syria Situation*. Accessed 24 March 2025. https://reporting.unhcr.org/operational/situations/syria-situation

[225] International Rescue Committee. (2024). *Syria: deepening economic crisis compounds conflict misery, as Syria crisis enters its fourteenth year and humanitarian needs reach unprecedented levels, warns the IRC*. Press release. Accessed 24 March 2025. https://www.rescue.org/press-release/syria-deepening-economic-crisis-compounds-conflict-misery-syria-crisis-enters-its

[226] UNHCR. (2025). *Global Report 2024 - Situation overview: Syria situation.* Accessed 30 July 2025. *https://www.unhcr.org/sites/default/files/2025-06/Syria%20GR2024%20Situation%20Summary%20v3.pdf*

[227] T. Perosa, Q. Tsui and S. Singler. (July 2023). BIOMETRICS IN THE HUMANITARIAN SECTOR. The Engine Room. Accessed 28 March 2025. https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf

[228] J. Wright and A. Verity. (2020). *Artificial Intelligence Principles for Vulnerable Populations in Humanitarian Contexts*. Digital Humanitarian Network. Accessed 24 March 2025.

https://app.box.com/s/df04s4tznhkjbak88jqurlwn5dyywlp3?,&source=aw&utm_medium=affiliate&utm_source=AWIN&utm_theme=AlwaysOnDigital&id=7010e000001LP9U&utm_campaign=85386&utm_content=0

[229] M. Moussa. (25 October 2024). Interview with author.

[230] M. Speier. (25 October 2024). Interview with author.

[231] A. Napolitano. (2023). *Artificial Intelligence: The New Frontier of the EU's Border Externalisation Strategy*. EuroMed Rights. Accessed 24 March 2025.

https://euromedrights.org/wp-content/uploads/2023/07/Euromed_AI-Migration-Report_EN-1.pdf

[232] Ibid.

[233] PICUM. (11 April 2024). *The EU Migration Pact: a dangerous regime of migrant surveillance.* PICUM blog. Accessed 24 March 2025. https://picum.org/blog/the-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance

[234] PICUM. (4 April 2024). *A dangerous precedent: how the EU AI Act fails migrants and people on the move*. PICUM blog. Accessed 24 March 2025. https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move

[235] A. Abrougui. (2024). *Position Paper on the European Union's AI Act and its Implications for Palestinian Digital Rights*. 7amleh. Accessed 24 March 2025. https://7amleh.org/storage/Position%20Paper%20on%20the%20European%20Union%E2%80%99s%20AI%20Act%20and%20its%20Implications%20for%20Palestinian%20Digital%20Rights%20.pdf

[236] M. Fatafta. (4 December 2024). Interview with author.

[237] Ibid.

[238] European Ombudsman. (28 November 2022). *Decision on How the European Commission Assessed the Human Rights Impact before Providing Support to African Countries to Develop Surveillance Capabilities (Case 1904/2021/MHZ)*. Accessed 24 March 2025.

https://www.ombudsman.europa.eu/en/decision/en/163491

[239] S. Ren and A. Wierman. (15 July 2024). *The Uneven Distribution of AI's Environmental Impacts*. Harvard Business Review. Accessed 24 March 2025.

https://hbr.org/2024/07/the-uneven-distribution-of-ais-environmental-impacts

[240] A. Eck. (2024). *Mapping Tech Companies*, op. cit.

[241] A. El Masri. (22 October 2024). Interview with author.

[242] A+ Alliance. (n.d.). *The Middle East and North Africa Hub*. Accessed 24 March 2025. https://aplusalliance.org/fair-middle-east-and-north-africa

[243] A+ Alliance. (22 April 2024). *The Network of Arab Women in AI (NAWAI) is pioneering feminist data research in MENA languages*. Accessed 10 February 2025. https://aplusalliance.org/the-network-of-arab-women-in-ai-nawai-is-pioneering-feminist-data-research-in-mena-languages

[244] A. Kawash. (n.d.). *Tatreez Garden*. Accessed 14 February 2025. https://ameerakawash.com/tatreez-garden

[245] A. Kawash. (8 November 2024). Interview with author.

[246] SinaLab. (n.d.). *Resources*. Accessed 14 February 2025. https://sina.birzeit.edu/resources/index.html

[247] M. Jarrar. (27 November 2024). Interview with author.

[248] SnaLab. (2025). *Nakba-NLP 2025: The 1st International Workshop on Nakba Narratives as Language Resources*. Accessed 24 March 2025. https://sina.birzeit.edu/nakba-nlp

[249] M. Jarrar. (27 November 2024). Interview with author.

[250] Meedan. (2 March 2023). *Meedan impact story: using AI to investigate weapons trafficking and human rights violations*. Meedan blog. Accessed 10 February 2025. https://meedan.com/post/meedan-impact-story-using-ai-to-investigate-weapons-trafficking-and-human-rights-violations

[251] D. Saber. (24 October 2024). Interview with author.

[252] "Artificial general intelligence (AGI) aims to replicate human cognitive capabilities across domains, setting the stage for transformative societal and economic impacts, particularly in areas involving human decision-making and adaptive reasoning". See: R. Raman, R. Kowalski, K. Achuthan, et al. (2025). *Navigating artificial general intelligence development: societal, technological, ethical, and brain-inspired pathways*. Sci Rep 15, 8443 (2025). https://doi.org/10.1038/s41598-025-92190-7

About Oxfam

Oxfam is a global movement of people who are fighting inequality to end poverty and injustice. We are working across regions in more than 70 countries, with thousands of partners, and allies, supporting communities to build better lives for themselves, grow resilience and protect lives and livelihoods also in times of crisis. Please write to any of the agencies for further information or visit www.oxfam.org.

Oxfam America (www.oxfamamerica.org)
Oxfam Aotearoa (www.oxfam.org.nz)
Oxfam Australia (www.oxfam.org.au)
Oxfam-in-Belgium (www.oxfamsol.be)
Oxfam Brasil (www.oxfam.org.br)
Oxfam Canada (www.oxfam.ca)
Oxfam Colombia (www.oxfamcolombia.org)
Oxfam France (www.oxfamfrance.org)
Oxfam Germany (www.oxfam.de)
Oxfam GB (www.oxfam.org.uk)
Oxfam Hong Kong (www.oxfam.org.hk)
Oxfam Denmark (www.oxfam.dk)
Oxfam India (www.oxfamindia.org)
Oxfam Intermón (Spain) (www.oxfamintermon.org)
Oxfam Ireland (www.oxfamireland.org)
Oxfam Italy (www.oxfamitalia.org)
Oxfam Mexico (www.oxfammexico.org)
Oxfam Novib (Netherlands) (www.oxfamnovib.nl)
Oxfam Québec (www.oxfam.qc.ca)
Oxfam South Africa (www.oxfam.org.za)
Oxfam KEDV (www.kedv.org.tr)
Oxfam Pilipinas (www.oxfam.org.ph)