Position Paper on the European Union's AI Act and its Implications for Palestinian Digital Rights

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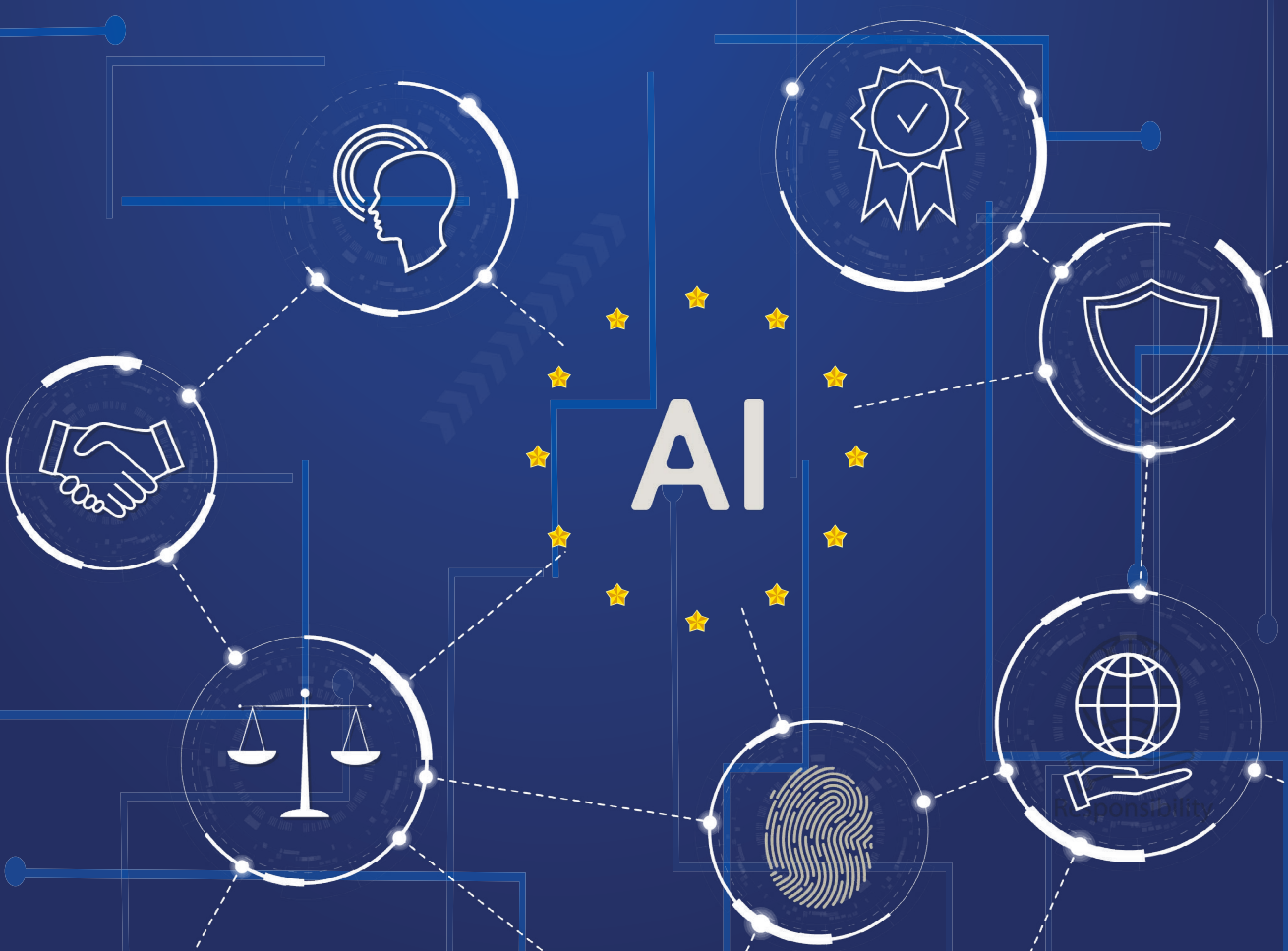
7amleh - The Arab Center for the Advancement of Social Media

The European Union's AI Act and its Implications for Palestinian Digital Rights

Author: Afef Abrougui

Designer: Amal Shoufany

Acronyms

- AI – Artificial Intelligence
- AI Act – Artificial Intelligence Act
- CSOs – Civil Society Organizations
- CSDDD – Corporate Sustainability Due Diligence Directive
- DSA – Digital Services Act
- EU – European Union
- FRIA – Fundamental Rights Impact Assessment
- GPAI – General Purpose AI
- HRDs – Human Rights Defenders
- ICJ – International Court of Justice
- SMEs – Small and medium-sized enterprises

Executive summary

This analysis of the EU AI Act[1] falls under 7amleh's policy work that investigates the intricate relationship between the Israel-Palestine context and European Union (EU) legislation, with a focus on their extraterritorial impacts on Palestinian human rights. This paper follows another, published in April 2024,[2] on the extraterritorial impacts of the Digital Services Act (DSA). Its objective is to dissect how the Act interferes with the fundamental human rights of Palestinians and risks emanating from the employment of AI in the Israel-Palestine context. It builds on a previous 7amleh study titled, "Impacts of AI Technologies on Palestinian Lives and Narratives,"[3] which identified four categories of AI systems that pose risks to human rights in Palestine: systems used in content creation, content moderation and curation, surveillance and automated warfare. AI systems used in content moderation and curation are excluded from this analysis since they largely fall under the scope of the DSA.

---

1. Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

2. Itxaso Domínguez de Olazábal, "Palestinian Digital Rights and the Extraterritorial Impact of the European Union's Digital Services Act," 7amleh, April 2024, https://7amleh.org/storage/Advocacy%20Reports/English%207amleh.pdf.

3. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

Our analysis found that the EU AI Act has a number of serious shortcomings that will only further exacerbate violations of Palestinian human rights, by Israel in the occupied Palestinian territory, and in the EU. In particular, as a result of the Act's limited scope, EU companies are not bound by its rules and safeguards when they sell their AI systems, even when they present high risks, abroad, including to Israel. The Israeli government deploys AI systems to aid its occupation of the occupied Palestinian territory and control the movements of Palestinians and subject them to invasive surveillance.

Additionally, exemptions in the Act for the use of high-risk AI systems by law enforcement and migration authorities risk exacerbating the surveillance and restrictions on Palestinians and advocates of Palestinian human rights in an increasingly hostile environment for Palestine advocacy and activism in the EU.

Finally, while the Act sets transparency and risk assessment requirements for GPAI, including Generative AI, it remains to be seen if this will have any ripple effects beyond the EU.

Introduction

The European Union's AI Act, adopted by the European Parliament on March 13, 2024, has been hailed as a "landmark" law[4] for being the world's first comprehensive legal framework to regulate artificial intelligence.[5] It prohibits AI systems which present unacceptable risks and places a number of safeguards for systems with high-risk. It also regulates General Purpose AI (GPAI) models, including Generative AI.

Palestinians are on a daily basis subjected to invasive technologies and AI systems deployed by Israel to restrict their fundamental rights, including their rights to privacy, nondiscrimination and movement. Since the start of the Israeli war on Gaza, more evidence has emerged of Israel's use of automated warfare tactics.[6] The Israeli army has also stepped up its use of facial recognition,[7] which it has long deployed in the occupied West Bank.[8] The

---

4. "Artificial Intelligence Act: MEPs adopt landmark law," European Parliament, March 13, 2024, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law.

5. Cynthia Kroet, "As the EU AI Act enters into force, focus shifts to countries' oversight appointments," Euronews, March 12, 2024, https://www.euronews.com/next/2024/03/12/as-ai-act-enters-into-force-focus-shifts-to-countries-oversight-appointments.

6. Marwa Fatafta and Daniel Leufer, Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes, Access Now, May 9, 2024, https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/.

7. Sheera Frenke, "Israel Deploys Expansive Facial Recognition Program in Gaza" The New York Times, March 27, 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html?unlocked_article_code=1.0k0.HWqW.XPDoFh0BK_ye&smid=url-share

8. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

Israeli military industrial complex is notorious for its development, deployment, and export of such invasive technologies, and the occupied Palestinian territory has long been known as a testing ground for the latest tech and weapons.[9] Israel also imports technologies that have been known to aid the Israeli occupation and dispossession of Palestinians, including from companies based in the EU.

The objective of this paper is to illustrate potential implications of the EU AI Act for Palestine and Palestinian human rights, with a focus on areas of AI deployment that present the most severe risks to Palestinians such as those deployed for surveillance and law enforcement purposes and those deployed in automated warfare and migration areas.

Desk research and legal analysis of the EU AI Act were used to illustrate the Act's limitations and potential implications, and the paper was guided by a number of research questions that were identified beforehand by 7amleh:

- How do the prohibitions and obligations outlined in the EU AI Act, especially concerning high-risk AI systems, align with or address the challenges faced by Palestinians in the use of AI, such as in militarized applications and surveillance systems?

- In what ways does the risk-based approach of the EU AI Act account for the diverse impact of AI on Palestinian digital rights, considering both high-risk scenarios and low-risk applications like generative AI tools?

- How do the transparency requirements and enforcement mechanisms of the EU AI Act contribute to accountability in the deployment of AI technologies in contexts affecting Palestinians?

- What potential gaps or limitations exist in the EU AI Act that may require additional considerations or adaptations to effectively safeguard Palestinian digital rights?

Two additional interviews with an EU policy expert and an AI expert were conducted to consolidate these findings and recommendations. The experts are Itxaso Domínguez de Olazábal, EU policy advisor at the European Digital Rights network (EDRi), and Meredith Veit, technology and human rights researcher at the Business and Human Rights Resource Centre (BHRRC).

The paper concludes by presenting recommendations for EU policymakers, CSOs and companies that provide and deploy AI systems, particularly EU companies exporting to Israel and companies that provide and deploy Generative AI models.

9. Antony Loewenstein, "Q&A with Antony Loewenstein, author of The Palestine Laboratory," Verso Books, October 25, 2023, https://www.versobooks.com/blogs/news/q-a-with-antony-loewenstein-author-of-the-palestine-laboratory.

Overview: EU AI Act in a nutshell

The Act defines an 'AI system' as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."[10] It sets rules and requirements for AI systems based on risk defined as "the combination of the probability of an occurrence of harm and the severity of that harm."[11]

Prohibited AI systems

The Act approaches the categorization of AI systems from a risk angle. AI systems and practices with unacceptable risk are prohibited. These include any AI system that "deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques," and "exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation," " with the objective, or the effect of materially distorting the behaviour" of persons. It also bans social AI systems used for social scoring and "the untargeted scraping of facial images from the internet or CCTV footage" to create or expand facial recognition databases.[12]

Other systems such as emotion recognition systems and facial recognition are only partially banned,[13] and when they are not banned, they are considered high-risk.[14]

The Act does not apply to the use of AI systems for military, defence, or national security despite dangerous human rights risks emanating from the use of AI in automated warfare.[15] In fact, Israel's war on Gaza has exposed the use of AI systems by the Israeli army to select targets for killings[16] and commit "domicide" (massive, arbitrary destruction of civilian

10. Article 3, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/ TA-9-2024-0138_EN.pdf.

11. Ibid.

12. "Chapter II: Prohibited Artificial Intelligence Practices," Artificial Intelligence Act, European Parliament, https:/ www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

13. Ibid.

14. Article 6 and Annex III, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/ doceo/document/TA-9-2024-0138_EN.pdf.

15. Article 2, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/ TA-9-2024-0138_EN.pdf.

16. Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza," +972 Magazine, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

housing).[17] The deployment of such systems exacerbated the high casualty rate among civilians. In a 15 April statement, a group UN experts said: "If proven true, the shocking revelations of the use of AI systems by the Israeli army such as "Gospel", "Lavender" and "Where›s Daddy?", combined with lowered human due diligence to avoid or minimize civilian casualties and infrastructure, contribute to explaining the extent of the death toll and home destruction in Gaza."[18]

High-Risk AI

For systems that pose "high-risk", developers and deployers have to comply with a number of requirements and additional safeguards. Some of these systems include those that Israel regularly uses to control Palestinians, control their movements, and violate their fundamental rights such as facial recognition and predictive policing.[19]

The Act considers "high-risk" AI systems any system that is a safety component or a safety product and required to undergo conformity assessment under EU laws and systems listed under Annex III.[20] These include the use of biometrics in AI systems, AI systems used as part of safety components in the management and operation of critical infrastructure (such as digital infrastructure, the supply of water and gas, etc.) systems used in education and vocational training "to determine access or admission," "to evaluate learning outcomes," etc. in employment, workers' management and access to self-employment, and systems determining access to and enjoyment of essential private services and essential public services and benefits such as those used to evaluate "the eligibility of natural persons for essential public assistance benefits and services, including healthcare."[21] A range of systems used for law enforcement purposes, migration, asylum, and border control management and for administration of justice and democratic processes are also considered high-risk. These include systems used "for the examination of applications for asylum, visa, or residence permits" and "AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution."[22]

---

17. "Gaza: UN experts deplore use of purported AI to commit 'domicide' in Gaza, call for reparative approach to rebuilding," OHCHR, April 15, 2024, https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call.

18. Ibid.

19. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

20. Article 6 and Annex III, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

21. Annex III, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

22. Ibid.

The Act places requirements for the development and deployment of high-risk AI systems including risk management "throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating," "data governance and management practices appropriate for the intended purpose of the high-risk AI system," ensuring human oversight measures that are "commensurate with the risks, level of autonomy and context of use of the high-risk AI system."[23] Before a high-risk AI system is placed on the market or put to service, its technical documentation should be drawn to demonstrate that the system complies with the requirements and to provide authorities with "the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those requirements." High-risk AI systems should be "designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately" and providers should accompany their systems with "instructions for use in an appropriate digital format or otherwise that include concise, complete, correct, and clear information that is relevant, accessible, and comprehensible to deployers."[24]

Under article 26, deployers are required to "assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support" and "immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities" of serious incidents.[25] Under article 27, public authorities or private entities providing public services are required to conduct FRIAs to assess the human rights impacts of the AI systems they deploy. These assessments will include the categories of persons and groups likely to be affected by the systems and "the specific risks of harm likely to have an impact" in addition to "a description of the implementation of human oversight measures."[26] However, deployers in this case are only required to detail mitigation measures when risks materialize not prior to that.

General-Purpose AI (GPAI) and Generative AI

The regulation of Generative AI in the Act falls under General Purpose AI (GPAI), defined as "an AI model…that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."[27] In recent

---

23. "Chapter III, Section 2: Requirements for High-Risk AI Systems," Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

24. Ibid.

25. Article 26, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

26. Article 27, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

27. Article 3, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

years, a wide range of these systems have become available to the general public. This is particularly the case with Generative AI such as OpenAI's ChatGPT and Google DeepMind's Gemini (formerly Bard), models that generate text, video, image, audio, and code, in response to prompts from users. While these tools are considered "low-risk", they have previously been shown to perpetuate anti-Palestinian bias,[28] which further risks undermining anti-occupation narratives and the historical, colonial, and political factors that have been responsible for the ongoing dispossession of the Palestinian people.

The Act places a number of transparency obligations on providers and deployers of GPAI, and additional obligations are placed on general-purpose AI with "systemic risk." Models pose a systemic risk if they have "high impact capabilities."[29] This is determined according to a set of criteria determined by the Act including the number of parameters of the model, the quality or size of the data set, the amount of computation used for training the model, and the number of end-users.[30]

Governance and remedy

Regulation of AI is conducted at Union level through the European Commision and national competent authorities at country level. An AI Office at the Commission will be established and will be tasked with "contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models."[31] The Office has the power to conduct evaluations of GPAI models to assess compliance and assess systemic risks. The Act also establishes a European Artificial Intelligence Board, made up of one representative per each Member State to "advise and assist the Commission and the Member States" in the Act's "consistent and effective application." National competent authorities are designated by each Member State to implement the Act.[32]

Under article 85, "any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit reasoned complaints to the relevant market surveillance authority." In article 86, the Act prescribes the right to explanation for a person "subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system."

28. Ameera Kawash, "What a cat in a keffiyeh reveals about AI's anti-Palestinian bias," +972 Magazine, April 25, 2023, https://www.972mag.com/ai-bias-palestinian-cat-keffiyeh/.

29. Article 51, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

30. "Annex XIII: Criteria for the Designation of General Purpose AI models with Systemic Risk," Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

31. Article 64, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

32. Article 65, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

Analysis

The Act's application scope fails to regulate the export of dangerous systems used by Israel

The Act only applies to those providing and deploying AI systems in the Union, including importers and distributors, providers, and deployers of AI systems, regardless of where they are based.

In this sense, companies that are based in the EU but export their systems outside the Union, including to Israel, are not bound by the Act's safeguards, even when the systems they export are banned or considered high-risk under EU law. As a result, dangerous systems such as facial recognition, predictive policing, emotion recognition and those used in the automation of warfare can be sold by EU companies to the Israeli government or Israeli companies without adequate safeguards and scrutiny to prevent violations against Palestinians.

Israel deploys a range of AI technologies to facilitate the occupation of the Palestinian territory and facilitate its control over Palestinians.[33] The ongoing Israeli war on Gaza has further exposed Israel's automated warfare tactics and their infringement on Palestinans' most basic rights including to life, security, protection from violence, and collective punishment. During the war, for instance, Israel has been using machine learning to select military targets and kill suspected militants. This automation, without proper human diligence, is believed to have contributed to the high number of civilian casualties, particularly women and children.[34] Palestinians in the West Bank are also subjected to automated weapons.[35]

Israel, a global leader in the development, deployment and exportation of military surveillance tech,[36] has for decades subjected Palestinians to invasive surveillance that infringes on their fundamental rights to privacy, freedom of expression and information, freedom of movement, and the right to protest and assembly. That surveillance is becoming

33. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

34. "Reported impact snapshot | Gaza Strip (5 June 2024)," OCHA, https://www.ochaopt.org/content/reported-impact-snapshot-gaza-strip-5-june-2024.

35. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

36. Antony Loewenstein, "Q&A with Antony Loewenstein, author of The Palestine Laboratory," Verso Books, October 25, 2023, https://www.versobooks.com/blogs/news/q-a-with-antony-loewenstein-author-of-the-palestine-laboratory.

more reliant on AI. In the West Bank, facial recognition is deployed to control Palestinians' movements and most recently Israel expanded the use of facial recognition to Gaza allegedly to identify suspected militants despite the inaccuracies and intrusiveness of these technologies.[37]

Prior to the Act's adoption, civil society organizations have been calling for the Act to be applied to companies exporting outside the Union. In a statement dated April 3, 2024, a coalition of digital, human rights, and social justice groups described the exclusion of exporters to non-EU countries from the safeguards and requirements of the Act as "a huge risk:" "The Act does not stop EU-based companies from exporting AI systems which are banned in the EU, therefore creating a huge risk of violating rights of people in non-EU countries by EU-made technologies that are essentially incompatible with human rights. Additionally, the Act does not require exported high-risk systems to follow the technical, transparency, or other safeguards otherwise required when AI systems are intended for use within the EU, again risking the violation of rights of people outside of the EU by EU-made technologies."[38]

Some of the technologies Israel deploys to aid its occupation of Palestinian land and control Palestinians and violate their fundamental human rights are imported from Europe. For instance, CCTV cameras made by Dutch company TKH Security[39] and Italian company Videotec[40] were previously documented to be in use by Israel in Israeli occupied East Jerusalem. The cameras support a wide surveillance infrastructure powered with facial recognition that subjugate Palestinians to constant surveillance and control their freedom of movement.

Several other EU-based technology companies are conducting business in Israel and with the Israeli government.[41] Some of these companies provide AI solutions or technologies that deploy AI systems, although it remains unclear to what extent they provide such systems to the Israeli government or companies and other entities that contribute to the occupation and violations against Palestinians.

---

37. Sheera Frenke, "Israel Deploys Expansive Facial Recognition Program in Gaza" The New York Times, March 27, 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html?unlocked_article_code=1.0k0.HWqW.XPDoFh0BK_ye&smid=url-share.

38. "EU's AI Act fails to set gold standard for human rights," EDRI, April 3, 2024, https://edri.org/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf.

39. "Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid," Amnesty, May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

40. "Videotec," Who Profits, Undated, https://www.whoprofits.org/companies/company/6171?6171-2.

41. "Switched off: Tech company opacity & Israel's war on Gaza," Business & Human Rights Resource Centre, April 18, 2024, https://www.business-humanrights.org/en/from-us/briefings/tech-sector-opt-analysis-2024/.

National security and law enforcement exceptions threaten the fundamental rights of Palestinian and pro-Palestine campaigners in the EU

The Act establishes dangerous exceptions for the deployment of AI systems for national security and law enforcement purposes. Despite calls by civil society to completely ban invasive systems such as facial recognition, predictive policing, and emotion recognition,[42] the EU categorized them in the Act as "high risk" and allowed their use by law enforcement.

For instance, the Act bans AI emotion recognition systems in the workspace and educational institutions but allows such systems "for medical or safety reasons."[43]

When it comes to remote biometric identification (RBI) law enforcement are allowed greater leeway. The use of 'real-time' remote biometric identification systems (live facial recognition) is allowed in publicly accessible spaces for the purposes of law enforcement," "when such use is "strictly necessary," for three objectives: 1) "the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons," 2) "the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack," and 3) the localisation or identification of a person for committing a serious offence such as human trafficking, terrorism, child sexual exploitation and rape.[44]

While in objectives 1 and 3, live facial recognition is used in the targeted search and localization of specific persons, the second objective provides room for interpretation and can potentially be abused under the pretext of security and counter-terrorism.

Additionally, the Act did not ban retrospective facial recognition (post remote biometric identification system in the text of the law), which are used to identify people after the fact. Rights groups warn that these technologies are as invasive as live facial recognition[45] and also disproportionately affect people of color.[46]

---

42. "EU's AI Act fails to set gold standard for human rights," EDRI, April 3, 2024, https://edri.org/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf.

43. Article 5, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

44. Ibid.

45. "EU's AI Act fails to set gold standard for human rights," EDRI, April 3, 2024, https://edri.org/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf.

46. Ella Jakubowska, Hajira Maryam and Matt Mahmoudi, "Retrospective facial recognition surveillance conceals human rights abuses in plain sight," Euronews, April 14, 2023, https://www.euronews.com/2023/04/14/retrospective-facial-recognition-surveillance-conceals-human-rights-abuses-in-plain-sight.

Other high risk AI systems that law enforcement can deploy are polygraphs, predictive policing, and crime prediction systems to assess "the risk of a natural person becoming the victim of criminal offenses," "the reliability of evidence in the course of the investigation or prosecution of criminal offenses," and "the risk of a natural person offending or re-offending," and "personality traits and characteristics or past criminal behavior of natural persons or groups."[47]

All these systems are prone to abuse and being inaccurate given existing biases and discrimination towards Muslims[48] and Arabs in Europe,[49] including Palestinians. The AI Act only risks increasing their profiling. Additionally, some of the safeguards that are established by the law are not applicable to law enforcement. In fact, law enforcement are exempted from publishing the details of the systems they use in a public database, further eroding accountability for their use of these systems.[50] And in an even more dangerous move, the EU included a national security exemption in the Act with article 2.3, stating: "This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence, or national security purposes, regardless of the type of entity carrying out those activities. This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence, or national security purposes, regardless of the type of entity carrying out those activities."

The blanket and broad exemption means that governments can invoke national security to do away with any of the safeguards established by the Act in the deployment by public authorities of AI systems that could infringe on people's fundamental rights such as facial recognition and predictive policing.

The use of these systems by law enforcement with minimal to no safeguards will only further erode the ability of campaigners and protesters in the EU to act in support of Palestine and Palestinian human rights. This is particularly worrisome given the sweeping restrictions on their rights to protest and assembly, as well as freedom of expression in the war on Gaza. For example, on April 13, German police banned a three-day pro-Palestine conference that sought to draw attention to Israel's ongoing genocide in Gaza

---

47. "Annex III: High-Risk AI Systems," Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

48. "Mapping anti-Muslim sentiment in Europe," Euractiv, December 2022 - January 2023, https://en.euractiv.eu/wp-content/uploads/sites/2/special-report/Mapping-anti-Muslim-sentiment-in-Europe-V4.pdf.

49. "Intolerance and discrimination against Arabs and Muslims: Statement by Mr. Githu Muigai, Special Rapporteur on contemporary forms of racism, racial, discrimination, xenophobia and related intolerance," OHCHR, October 14, 2009, https://www.ohchr.org/en/statements/2010/09/intolerance-and-discrimination-against-arabs-and-muslims-statement-mr-githu.

50. Article 71, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

on the grounds of false accusations of antisemitism.[51] Dr Ghassan Abu Sitta, one of the conference's speakers was banned from entering Germany and attending the event, and the General Federal Police placed on him a one-year Schengen-wide travel ban, preventing him from traveling to 29 countries across Europe.[52] The ban was later overturned by a court in Berlin. In another example, student protesters, inspired by their peers at U.S. campuses, were met with police violence and arrests across Europe when they set up encampments and organized demonstrations to demand their universities disclose their partnerships with Israeli institutions and divest from them.[53] Advocates have also previously been targeted with surveillance.[54] By failing to address the risks of AI systems deployed by law enforcement and banning the most invasive of these systems such as predictive policing and facial recognition, the EU AI Act risks further exacerbating the restrictions Palestinian and pro-Palestine advocates and protesters face in the EU.

While public authorities are required to perform an FRIA before they deploy a high-risk AI system, law enforcement authorities may be exempted from notifying the market surveillance authorities of the results of the assessments before first putting a system into use "upon a duly justified request (…) for exceptional reasons of public security or the protection of life and health of persons, environmental protection, or the protection of key industrial and infrastructural assets."[55] Additionally, law enforcement are not required to publicly disclose the results of the FRIAs.

Prosecutions and strategic litigation

The Act allows for the use of "AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution."[56]

---

51. "German police shut down pro-Palestinian conference," DW, April 13, 2024, https://www.dw.com/en/german-police-shut-down-pro-palestinian-conference/a-68810306.

52. "VICTORY FOR DR GHASSAN ABU SITTAH: ELSC and ICJP overturn Schengen-wide travel ban," European Legal Support center, May 15, 2024, https://elsc.support/news/victory-for-ghassan-abu-sittah-elsc-and-icjp-overturn-schengen-wide-travel-ban.

53. Ashifa Kassam and agencies, "Clashes and arrests as pro-Palestinian protests spread across European campuses," The Guardian, May 8, 2024, https://www.theguardian.com/world/article/2024/may/08/pro-palestine-student-protests-campuses-europe-arrests-police.

54. "Anti-Palestinian Surveillance in Germany: New Hearing in the Case of Dr Anna Younes," European Legal Support Center, May 15, 2024, https://elsc.support/news/victory-for-ghassan-abu-sittah-elsc-and-icjp-overturn-schengen-wide-travel-ban.

55. Article 27, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

56. Article 6 and Annex III, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

It remains to be seen how judicial authorities' use of AI systems to assist them will impact advocacy efforts in the EU after the Act comes into force. Activists, protesters, and advocates throughout the EU have been facing arrests and charges.[57] Civil society and campaigners have also been fighting some of these cases and restrictions[58] and engaging in strategic litigation in support of Palestinian self-determination. Cases have been brought up against EU governments for their arms export to Israel. In February 2024, three Dutch organizations won an appeal in court against the Dutch government for supplying Israel with F35 fighter jet parts,[59] and a similar lawsuit against the Danish National Police and the Ministry of Foreign Affairs was announced in March 2024.[60]

AI systems used by judicial authorities will not be taking decisions. However, given existing biases towards Palestine and Palestinians and intolerance towards criticism of Israel in Europe, if the systems reflect real-life biases, their interpretation of "facts and the law" will also be biased, and not favor the rights of Palestinians and pro-Palestinian rights advocates.

These systems are listed as high-risk by the Act and are thus subjected to the safeguards outlined earlier in the paper, including risk assessment, data management, governance, and transparency. Unlike law enforcement and migration authorities, judicial authorities are not exempted from registering the systems they use in a publicly available database and providing details such as their purposes, components and functions, data and inputs used by the systems, and their operating logics. In addition to FRIAs and their results, which will be made available to the public, this can help scrutinize the use of these systems by judicial authorities given potential risks to those on trial and those seeking judicial recourse.[61]

57. Jonathan Shamir, "An Anti-Palestinian Crackdown Across Europe," Jewish Currents, October 26, 2023, https://jewishcurrents.org/an-anti-palestinian-crackdown-across-europe.

58. "VICTORY FOR DR GHASSAN ABU SITTAH: ELSC and ICJP overturn Schengen-wide travel ban," European Legal Support center, May 15, 2024, https://elsc.support/news/victory-for-ghassan-abu-sittah-elsc-and-icjp-overturn-schengen-wide-travel-ban.

59. "Oxfam reaction to the Dutch court's decision to stop military exports to Israel," Oxfam International, February 12, 2024, https://www.oxfam.org/en/press-releases/oxfam-reaction-dutch-courts-decision-stop-military-exports-israel.

60. "Oxfam sues the Danish state to stop arms exports to Israel," Oxfam International, March 12, 2024, https://www.oxfam.org/en/press-releases/oxfam-sues-danish-state-stop-arms-exports-israel.

61. "Annex VIII: Information to be submitted upon the registration of high-risk AI systems in accordance with Article 49," Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

In migration areas, the Act fails Palestinian asylum seekers and people on the move

The EU AI Act allows the deployment of a range of systems used in areas of migration, asylum and border control management, and categorizes them as high risk. The AI Act, together with the new Pact on Migration and Asylum,[62] and the new Schengen Borders Code,[63] will only expand the use of invasive technologies and constitute a culmination of years of inhumane EU migration policies and measures.

This new more repressive framework, and its reliance on technology including AI, will only further marginalize and discriminate against people on the move, including Palestinians seeking asylum as a result of the war, Palestinians applying for EU residence or naturalization, and those simply seeking short entry to the Schengen area to speak and attend conferences and events or engage in advocacy at an EU level, such as journalists, human rights defenders, advocates, politicians, etc. According to the European Union Agency for Asylum (EUAA), the number of Palestinians applying for asylum increased in 2023 reaching nearly 11,600, a two-third increase from 2022.[64]

Some of the AI technologies whose usage will be normalized and expanded to control EU borders include lie detectors, which analyze facial movements to tell if a person is telling the truth or not, dialect recognition systems to verify if asylum applicants are telling the truth on where they are from, and facial recognition and automated systems that assess risks pertaining to security, irregular migration, and health by those intending to enter or entered the EU, and systems that examine applications for asylum, visa or residence permits. Additionally, law enforcement, as explained previously, have the power to use invasive AI systems such as emotion recognition and facial recognition to control borders.

In a statement, a coalition of human rights groups have expressed concerns about this new "dangerous regime of migrant surveillance" and its risks to privacy, freedom of movements, and the right to non-discrimination.[65]

This risks further exacerbating existing biases against Palestine and Palestinians and the association of pro-Palestine and anti-occupation advocacy with false accusations of "terrorism" and "anti-semitism." These false accusations have intensified since the start of the war on Gaza, with travel bans being imposed on those exercising their rights to freedom of expression and calling out Israeli crimes and violations, as was the case with the ban imposed by Germany on Dr. Ghassan Abu Sittah.

62. "The EU Migration Pact: a dangerous regime of migrant surveillance," PICUM, April 11, 2024, https://picum.org/blog/the-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance.

63. "Racial profiling key element in the new deal on the Schengen Borders Code," PICUM, February 7, 2024, https://picum.org/blog/racial-profiling-schengen-borders-code.

64. "EU received over 1.1 million asylum applications in 2023," EUAA, February 28, 2024, https://euaa.europa.eu/news-events/eu-received-over-1-million-asylum-applications-2023.

65. "The EU Migration Pact: a dangerous regime of migrant surveillance," PICUM, April 11, 2024, https://picum.org/blog/the-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance.

With the EU Act, those biases will be fed into automated systems that make decisions affecting fundamental human rights of crucial Palestinian voices and anti-occupation advocates, as well as those seeking asylum and safety and those speaking out against violations committed by Israel as it continues its war on Gaza. Yet, the safeguards for the use of these systems are lacking. As mentioned above, in addition to law enforcement, migration authorities are also exempted from registering information about the AI systems they use in a publicly available database. While they are required to conduct FRIAs, law enforcement, which play a fundamental role in border control and management, may be exempted from notifying the market surveillance authorities of the results of the assessments before first putting a system into use and are not required to publicly disclose the results of the FRIAs.

Will the EU Act's approach to general-purpose AI help set global standards for the industry?

The regulation of Generative AI in the Act falls under the scope of general purpose AI, defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

As with other providers of AI systems, EU-based providers of general-purpose AI that provide and sell their systems abroad are not covered by the new Act's rules. However, the Act applies to GPAI providers that are based outside the EU and provide their services in the EU, so these providers will need to abide by the Act's rules. It remains to be seen if these standards will have a ripple effect and be adopted by these providers as global standards, and what the impacts will be for Palestinian human rights. Big players in the field such as OpenAI and Microsoft, given their resources, may choose to adopt different standards in different markets, while for startups and smaller companies, abiding by these standards on a global level would be more cost efficient.

Generative AI tools which generate synthetic media like images, texts, videos, and audio in response to user prompts have previously been known to perpetuate biases against Palestinians and their stereotyping as a result of existing biases in the data sets.[66] These tools are also deployed to create propaganda and disinformation, as it has been the case during the ongoing war in Gaza, where all sides of the conflict deployed AI to deceive others and disinform.[67]

---

66. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

67. David Klepper, "Fake babies, real horror: Deepfakes from the Gaza war increase fears about AI's power to mislead," AP News, November 23, 2024, https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47.

For instance, Meta-owned WhatsApp's image generator repeatedly showed images of gun-toting children when prompted with the words 'Palestinian' and 'Muslim boy Palestinian'[68] and there were reports of OpenAI's ChatGPT providing misleading information and Google's Bard (before rebranding to Gemini) "shutting down" when prompted with questions related to Palestine.[69]

The Act requires GPAI models to "ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated" while "deployers of an AI system that generates or manipulates image, audio, or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated." When these provisions come into force, they can help stem the spread[70] by different parties of deep fakes and disinformation particularly around the Gaza war[71], at least in the EU. Since the start of the war on Gaza, the Israeli government has stepped up its propaganda campaigns to sway the public opinion, including in Europe, and drum up support for its war on Gaza, using graphic footage, targeted ads, and disinformation, including deep fakes.[72]

The Act also sets additional obligations for general-purpose AI with "systemic risk", including risk assessment, reporting "without undue delay serious incidents" to the authorities and adopting "adequate level of cybersecurity protection."[73] According to article 51 of the Act, a general-purpose AI model presents a systemic risk if "it has high impact capabilities," that is "when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}." The European Commission can also decide that a model presents systemic risks based on certain criteria such as the number of parameters of the model, the quality or size of the data set, the amount of computation used for training the model (measured in floating point operations), number of registered business users established in the EU (at least 10,000) and the number of registered end users.

68. Johana Bhuiyan, "WhatsApp's AI shows gun-wielding children when prompted with 'Palestine'," The Guardian, November 3, 2023, https://www.theguardian.com/technology/2023/nov/02/whatsapps-ai-palestine-kids-gun-gaza-bias-israel.

69. Meera Navlakha, "Google Bard, ChatGPT: Are AI chatbots suppressing information about Israel and Palestine?", Mashable, October 26, 2023, https://mashable.com/article/ai-chatbot-israel-palestine-chatgpt-google-bard.

70. Ameera Kawash, "Position Paper on Impacts of AI Technologies on Palestinian Lives and Narratives," 7amleh, February 2024, https://7amleh.org/2024/02/21/7amleh-releases-position-paper-on-ai-technologies-impact-on-palestinian-lives-and-narratives.

71. David Klepper, "Fake babies, real horror: Deepfakes from the Gaza war increase fears about AI's power to mislead," AP News, November 23, 2024, https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47.

72. Liv Martin, Clothilde Goujard and Hailey Fuchs, "Israel floods social media to shape opinion around the war," POLITICO, October 17, 2023, https://www.politico.eu/article/israel-social-media-opinion-hamas-war.

73. Article 51, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

Based on this criteria, the most influential Generative AI models like ChatGPT and Gemini will be considered systemic risk. The Commission will publish a list of general-purpose AI models with systemic risk, which can help the public, including Palestinian civil society and human rights groups, better scrutinize such models.

Risk assessment for GPAI models that pose systemic risk should include "a model evaluation…including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks." They should also "assess and mitigate possible systemic risks at Union level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk."[74]

---

74. Article 55, Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/ TA-9-2024-0138_EN.pdf.

Recommendations

Policymakers

· National governments and relevant authorities should go beyond the requirements of the Act to regulate exports of AI systems outside the EU especially to crisis or conflict zones. This includes mandating that Human Rights Impact Assessments (HRIAs) be conducted for AI technologies deployed outside the EU, ensuring that the rights of individuals in all regions are protected.

· In the implementation stage of the AI Act, policymakers and regulators should not cave in to the lobbying pressures of the private sector, particularly when setting implementation guidelines for high risk AI systems and GPAI that pose systemic risks and when reviewing assessments made by companies on whether their systems are high risk or not.

· Migration authorities that deploy AI systems to help them make decisions on visa, assylum, and residence applications should be transparent about the input of their data, and whether publicly available data, such as applicants' social media posts, feed those systems.

· When conducting FRIAs, public authorities should actively engage with civil society and communities that are likely to be the most disproportionately affected by their AI systems, particularly communities that face discrimination and bias, societal or institutional. They should also ensure that the data sets that train AI systems they deploy are adequately audited to minimize bias.

· EU Policymakers should expand the scope of the Corporate Sustainability Due Diligence Directive (CSDDD)[75] to cover smaller companies and tech startups. The directive requires "companies in scope identify and address adverse human rights and environmental impacts of their actions inside and outside Europe." However, it does not apply to SMEs even though such companies, particularly in the AI and technology field, can still get implicated in human rights harms and exporting technologies to Israel that can aid the occupation and violate the human rights of Palestinians.

Civil society

· CSOs should advocate on behalf of historically and currently marginalized groups and those facing discrimination in the EU, including Palestinian and pro-Palestinian rights advocates, in their engagement and with EU policymakers, the AI Office, and national

---

75. "Corporate sustainability due diligence," European Commission, Undated, https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en#which-companies-will-the-new-eu-rules-apply-to.

authorities to ensure that the design and deployment of AI systems do not further contribute to their marginalization and exacerbate harms that affect them.

- CSOs need to actively engage in the implementation stages of the Act, particularly with the EU Commission when setting implementation guidelines for high risk AI systems and GAPIs with systemic risk and with the AI Office to make sure it develops a comprehensive and robust questionnaire to guide the FRIAs that public authorities are required to conduct.

- CSOs and journalists should further investigate EU AI systems that enable the Israeli occupation and violations against Palestinians and contribute to the silencing of pro-Palestinian rights advocacy in the EU. In addition, they should further investigate how AI systems deployed by migration authorities discriminate against those on the move, specifically Palestinian migrants and asylum seekers. More evidence will not only help support general advocacy efforts but can inform FRIAs and push the public bodies conducting them to take appropriate risk mitigation and prevention measures.

Companies providing and deploying AI systems

- EU technology companies, regardless of their size, should conduct robust due diligence before exporting their AI systems outside the EU, to assess potential risks to human rights, and minimize or eliminate them altogether depending on the context. These include surveillance tech like facial recognition and video surveillance cameras, automated systems used in predictive policing, and other systems deployed by Israel to prevent Palesitnans from exercising their fundamental rights.

- Technology companies that already operate and do business in Israel or export their products there, regardless of their size and revenue, should also conduct human rights impact assessments to investigate whether their systems have been used in human rights violations and take appropriate mitigation actions.

- GPAI should conduct human rights impact assessments to assess how their systems contribute to and exacerbate anti-Palestinian bias at a time when Palestinians in Gaza are subjected to a "plausible" genocide per the ICJ ruling in the case brought up by South Africa against Israel.[76] They should also adopt the transparency and risk assessment measures required under the AI Act not only in the EU but globally to ensure that the rights of users and communities are equally protected everywhere.

---

76. "ORDER APPLICATION OF THE CONVENTION ON THE PREVENTION AND PUNISHMENT OF THE CRIME OF GENOCIDE IN THE GAZA STRIP (SOUTH AFRICA v. ISRAEL)," International Court of Justice, January 26, 2024, https://www.icj-cij.org/node/203447.