إصـدار زمـالـة مريـم أبو دقّـة

الهيـــمنة الرقمـية

الذكاء الاصطناعي والمراقبة والسلطة الرقمية في فلسطين وما بعدها

جامعة بيرزيت
BIRZEIT UNIVERSITY
معهد ابراهيم أبو لغد للدراسات الدولية
Ibrahim Abu-Lughod Institute of International Studies

حملة - المركز العربي لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for the Advancement of Social Media

الهيمنة الرقمية

الذكاء الاصطناعي والمراقبة والسلطة الرقمية في فلسطين وما بعدها

إصدار زمالة مريم أبو دقّة

زملاء البرنامج
إسلام الخطيب
أريس بشارة
سارة فتح الله
ميلودي سيباهبور
روان يوسف

المساهمات التحريرية والأكاديمية
مقدمة
جلال أبو خاطر — مدير السياسات في مركز حملة
باسل فراج — مدير معهد إبراهيم أبو لغد للدراسات الدولية، جامعة بيرزيت
المرشد الأكاديمي للبرنامج
إمطانس شحادة
منسق البرنامج
جلال أبو خاطر

ترجمة
مرسال ميديا

تصميم
نور سادات

تواصلوا معنا:

ialiis@birzeit.edu info@7amleh.org
ialiis.birzeit.edu www.7amleh.org

UpScrolled

في ذكرى الشهيدة مريم أبو دقّة
الصحفية الفلسطينية التي اغتالتها إسرائيل في غزة
25 آب 2025

يُهدى هذا الإصدار إلى روح الشهيدة مريم أبو دقّة، الصحفية الفلسطينية التي اغتالتها إسرائيل في غزة يوم 25 آب 2025، أثناء قيامها بواجبها المهني والأخلاقي في توثيق واقع الحياة الفلسطينية تحت الحصار والاحتلال وحرب الإبادة. وقد جسّد عملها الشجاعة والنزاهة والالتزام التي ميّزت الصحافة الفلسطينية لعقود طويلة.

تأتي تسمية هذه الزمالة تكريماً لمئات الصحفيين والإعلاميين والكتّاب والمصورين والرواة الفلسطينيين الذين دفعوا حياتهم ثمناً لنقل الحقيقة وحفظ الذاكرة الجماعية. فقد أسهمت جهودهم في ضمان استمرار توثيق التجربة الفلسطينية وإيصال أصوات الفلسطينيين وتطلعاتهم إلى العالم، رغم محاولات الطمس والإسكات والتدمير. وإذ نحيي ذكراهم، نؤكد أهمية إنتاج المعرفة والتوثيق وكشف الحقيقة بوصفها ركائز أساسية في نضالنا من أجل العدالة والكرامة الإنسانية.

مقدمة

يأتي نشر هذا الكتاب في وقت يتسم بتعاظم وتزايد العنف على نطاق عالمي، وتعميق العسكرة، وتطبيع الحروب في العديد من نواحي العالم. في فلسطين، تواصل إسرائيل بنشر وتفعيل نظام استعماري استيطاني يتميز بأشكال متعددة من العنف والتعذيب، من ضمنها حرب الإبادة على المجتمع الفلسطيني، وبشكل خاص على الفلسطينيين في قطاع غزة، في حين تصون نظام شامل للسيطرة على حيوات الفلسطينيين في جميع أنحاء تواجدهم. لا تتم الهيمنة الاسرائيلية بفعل القوة العسكرية والتكتيكات العنيفة المرئية فحسب، بل إنها تُمارس أيضًا من خلال آليات قانونية واقتصادية وتكنولوجية، والتي تتحكم وتقيد حركة الفلسطينيين، تُعيق الوصول إلى الموارد، تنتهج العنف، وتُكيل بهجوم عنيف على أي جهود للتعبئة والتنظيم السياسي والاجتماعي.

خارج فلسطين، يمتد نطاق العنف العسكري الإسرائيلي إلى لبنان، حيث عرّضت الانتهاكات الاسرائيلية للسيادة اللبنانية واحتلال أراضي لُبنان مُرفقة بهجمات وتوغلات عسكرية مُتكررة، الشعب اللبناني للعنف المتواصل، والتهجير والتشريد القسري، إضافة إلى تعريض سُبل عيش الشعب اللبناني للمخاطر والتهديدات شتى. في الوقت نفسه، تواصل الولايات المتحدة، في تحالف وثيق مع إسرائيل، ممارسة أشكال متعددة من الإكراه والضغط على إيران من خلال مزيج من الحرب الاقتصادية، بما في ذلك أنظمة العقوبات، إلى جانب التصعيدات العسكرية وأعمال العدوان التي تسهم في تعميق حالة عدم الاستقرار الإقليمي.

وتعكس هذه الديناميكيات العدوانية والعنيفة بصورة متزايدة نمطًا أوسع تتداخل فيه البنى التحتية للمراقبة، وأنظمة الاستخبارات القائمة على البيانات، وتقنيات الاستهداف المدعومة بالذكاء الاصطناعي في تشكيل العمليات العسكرية وتوسيع نطاقها عبر ساحات متعددة. وقد تجلّى ذلك في ضربات عسكرية شهدتها المنطقة مؤخرًا، بما في ذلك الضربة التي استهدفت مدرسة ميناب في إيران، حيث أُثيرت تساؤلات بشأن دور أنظمة الاستهداف المعززة بالذكاء الاصطناعي والمعلومات الاستخباراتية غير الدقيقة في التسبب بأضرار كارثية طالت المدنيين[1].

ومع ذلك، فإن هذه الديناميكيات العالمية تتخطى حدود منطقتنا. في الولايات المتحدة، يوصف سلوك هيئة إنفاذ قوانين الهجرة والجمارك (ICE) على نحو متزايد بأنه يشبه سلوك قوة شبه عسكرية.[2] من خلال أنظمة الاعتقال والاحتجاز المُوّسعة، ومنشآت وبنى التجسس التحتية، علاوة على الترحيل، تتعرض مجتمعات بأكملها، وخاصة المهاجرين والسكان المُصنّفون على أساس عُنصري، للتجريم والعنصرية والعنف المُمنهج. تعتمد البنى التحتية التي تُمكّن مثل هذه الأنظمة بشكل متزايد على تركيز البيانات الآخذ بالنمو، تكنولوجيا التنبؤ، وأنظمة تحليل قائمة على الذكاء الاصطناعي والتي عمدت شركات تقنية خاصة إلى تطويرها. وبالتالي، لم تعد الأسئلة المعنية باستخراج البيانات وجمعها، السلطة الرقمية المُركّزة، والتجسس بواسطة

1 كيفن تي بيكر، "حُمِّل الذكاء الاصطناعي مسؤولية قصف المدرسة الإيرانية، لكن الحقيقة أكثر إثارةً للقلق بكثير" صحيفة الجارديان، 26 مارس 2026، https://www.theguardian.com/news/2026/mar/26/ai-got-the-blame-for-the-iran-school-bombing-the-truth-is-far-more-worrying.

2 إريكا دي بروين، "ICE هيئة إنفاذ قوانين الهجرة والجمارك لا تبدو وتتصرف كقوة شبه عسكرية فحسب، بل إنها واحدة، مما يجعل من الصعب كبحها"، ذي كونفرسيشن، 28 كانون الثاني/ يناير 2026، https://theconversation.com/ice-not-only-looks-and-acts-like-a-paramilitary-force-it-is-one-and-that-makes-it-harder-to-curb-274580.

الذكاء الاصطناعي، أسئلة محصورة في فلسطين أو مناطق الاقتتال والاحتراب، بل إنها تُشكّل القضايا العالمية المعنية بصياغة أشكال الحوكمة والحدود والشرطة والعسكرة والحياة العامة.

في المملكة المتحدة، يُشير دمج شركات مثل بالانتير بشكل متعاظم في مؤسسات الدولة والبنية التحتية العامة، من خلال عقود عامة بقيمة 600 مليون جنيه إسترليني معنية بالرعاية الصحية، الشرطنة، والأنظمة العسكرية، من بين أمور أخرى إلى الانتشار العالمي وتطبيع هذه التقنيات بشكل يتعدى السياقات العسكرية الصريحة.[3] مُجتمعة، تعكس هذه الأمثلة حالة عالمية أوسع أمست فيها العسكرة والعنف من السمات التي تميّز عالمنا اليوم بشكل دائم، والتي تؤثر على المجتمعات المُهمشة الخاضعة للاحتلال والمُصنّفة على أساس عنصريّ، بشكل غير متناسب ومتفاوت. ومع ذلك، فإن ما يميّز الوقت الراهن ليس استمرار العنف الجسدي وحده، والذي يتجلى في الحرب، ومن خلال الاحتلال، الضم، والحصار، بل يتميّز أيضًا بالتوّسيع والانتشار السريع لأنظمة السيطرة والعنف المدعومة تكنولوجيًا والأقل بروزًا.

ما يظهر عبر هذه السياقات هو نمط مشترك وعميق العواقب: تسليح التقنيات المتقدمة لتمكين طرائق جديدة للتجسس والاستهداف والقتل والسيطرة. تُستخدم أنظمة الذكاء الاصطناعي بشكل متزايد لمعالجة كميات هائلة من البيانات، تصنيف وفرز الأفراد والسكان، التنبؤ بالسلوك، وتسهيل أشكال العنف والتجسس المُباشرة وغير المباشرة. لا ترافق هذه التقنيات العمليات العسكرية فحسب؛ بل إنها تعيد صياغة أشكال السلطة بالممارسة الفعلية في الحيّز العام، مما يُطيل يد الجهات الفاعلة الحكومية وغير الحكومية والشركات لتطال الجوانب الأكثر حميمية بالحياة اليومية. في الواقع، يوثق تقرير حديث صادر عن منظمة العفو الدولية، بعنوان «تكنولوجيا صنعتها بالانتير وبابل ستريت تشكّل تجسسًا يهدد الطلبة المتظاهرين المناصرين لفلسطين والمُهاجرين»، كيف تنشر السلطات الأمريكية أدوات تجسس مدعومة بالذكاء الاصطناعي لرصد واستهداف مهاجرين، «غير مواطنين»، والمدافعين عن حقوق الفلسطينيين.[4] تشهد تكنولوجيا طوّرتها شركات كـ «بالانتير تكنولوجيز» و «بابل ستريت» على النطاق الواسع لتجميع وتحليل البيانات الشخصية، تسهيل ممارسات التنميط العرقي على أساس عنصري، المتابعة والرصد، وتصنيف مجتمعات بأكملها، والاستخدام الوحشي لأنظمة العنف والتجسس والترحيل. توّسع هذه التقنيات إلى قطاعي الحوكمة المدنية والعامة يوضح الدمج المتزايد لأنظمة قائمة على الذكاء الاصطناعي في هياكل الحوكمة اليومية، وتطبيع التجسس واستخراج البيانات كممارسة إدارية عادية.

وبالمثل، أدمجت إسرائيل أنظمة الذكاء الاصطناعي في صميم أنظمتها العسكرية وأنظمة السيطرة على السكان. علاوة على تقنيات التعرّف على الوجوه المُوظفة على نطاق واسع في جميع أنحاء فلسطين المُحتلة لرصد تحركات الفلسطينيين والتحكم بها، كثّفت السلطات الإسرائيلية توظيف التقنيات القائمة على الذكاء

3 مات هاي، "بالانتير يواجه ردة فعل قاسية إزاء عقود حكومية بقيمة تفوق 600 مليون جنيه استرليني مع حكومة المملكة المتحدة"، BusinessChief، 30 نيسان/ أبريل 2026، https://businesschief.com/news/palantir-faces-backlash-over-600m-uk-government-contracts.

4 منظمة العفو الدولية، " الولايات المتحدة الأمريكية/عالميًا: تكنولوجيا شركتي بالانتير وبابل ستريت تشكّل تهديدات رقابية على الطلاب المحتجّين والمهاجرين المؤيّدين لفلسطين"، منظمة العفو الدولية، 21 آب/ أغسطس 2025، https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/

الاصطناعي عند إطلاقها لآليات العنف الإبادي والتجسس.[5] وقد لعبت شركات التكنولوجيا الكبرى - منها جوجل وأمازون - دورًا مهمًا في هذه الصيرورة،[6] وبشكل خاص من خلال مشروع «نيمبوس» على سبيل المثال،[7] الذي يوّفر البنية التحتية للحوسبة السحابية وقدرات تعلم الآلة للهيئات الحكومية والعسكرية الإسرائيلية. بالمقابل، وُظفت أنظمة الاستهداف المدعومة بالذكاء الاصطناعي - أمثال «لافندر» (Lavender) و»ذي جوسبل» (The Gospel) و»ويرز دادي» (Where›s Daddy) لتسريع عمل آليات التجسس والهجمات العسكرية على الفلسطينيين مما ساعد النظام الإسرائيلي بتوسيع رقعة حرب الإبادة الجماعية ضد السكان الفلسطينيين والتجسس عليهم.

دَمج الذكاء الاصطناعي في الحرب واضح أيضًا في الحرب الروسية - الأوكرانية المستمرة. هناك، أصبحت ساحة المعركة حلبة اختبار التقنية الناشئة، بما في ذلك المُسيرّات المُستقلة الذاتية، أنظمة الاستطلاع المدعومة بالذكاء الاصطناعي، والمنصات الروبوتية المُصممة للتجسس، إزالة الألغام والدعم القتالي.[8] تُشير هذه التطوّرات إلى تحوّل أوسع ومتزايد نحو أشكال الحرب الآلية، حيث تساعد السيرورات الخوارزمية بشكل متزايد في المواقع الجغرافية التي ينتشر فيها العنف وتعيد تشكيلها.

يأتي هذا الكتاب في إطار هذا المشهد سريع التطوّر وثيق الارتباط، حيث تحتل تقنيات التجسس القائمة على الذكاء الاصطناعي الصدارة، وتستمر بالتأثير على المشهد السياسي والاجتماعي بفاعلية. يسعى الكتاب إلى معاينة تشابك الذكاء الاصطناعي وأنظمة التجسس وتأثير الشركات في صياغة وتشكيل نُظم العنف والسيطرة المُعاصرة في فلسطين وخارجها برؤية نقدية. لا يتعامل الكتاب مع هذه القضايا كظواهر معزولة، بل كمكونات لبُنية عالمية يرتبط فيها الابتكار التكنولوجي ارتباطًا وثيقًا بالعنف والعسكرة والإبادة الجماعية وتكنولوجيا التجسس.

يُمثل هذا المنشور تتويجًا لأول مجموعة من أبحاث الزمالة من تنظيم «حملة» – المركز العربي لتطوير الإعلام الاجتماعي، وقد عمل على جمعه وإعداده جلال أبو خاطر. تلق برنامج الزمالة الذي يحمل اسم مريم أبو دقّة، تكريمًا للصحافية الفلسطينية التي استشهدت في غزة أثناء آب/ أغسطس 2025، ما يقرب من 140 طلبًا، مما يعكس أهمية الموضوعات التي سعت إلى معالجتها وكشفها. خفي أعقاب صيرورة اختيار جادة وصارمة، وقع الاختيار على خمس دراسات زمالة ودعمها من خلال الإرشاد المستمر.

من الجدير بالذكر أن جميع الزمالات التي وقع عليها الاختيار هي لباحثات نساء. تعكس هذه النتيجة القوة والعمق والدقة التحليلية التي تظهر في أعمالهن. ثلاث من دراسات الزمالة من تأليف نساء فلسطينيات، ترتكز كل منها على واقع سياسيّ متميّز، لكن جميعها مرتبطة: القدس وحيفا وسياق اللاجئين الفلسطينيين في

5 أمبر رحمان، " دور الذكاء الاصطناعي في حملة الإبادة الجماعية التي يشنها الاحتلال الاسرائيلي ضد الفلسطينيين"، مؤسسة الدراسات الفلسطينية، 16 تشرين الأول/ أكتوبر 2024، https://www.palestine-studies.org/ar/node/1656285

6 مروة فطافطة، "الذكاء الاصطناعي من أجل الحرب: تواطؤ شركات التكنولوجيا مع الاحتلال الإسرائيلي وجرائمه"، الشبكة: شبكة السياسات الفلسطينية، 26 تشرين الأول/ أكتوبر 2025، https://al-shabaka.org/briefs/الذكاء-الاصطناعي-من-أجل-الحرب-تواطؤ-شركات-التكنولوجيا-مع-الاحتلال-الإسرائيلي-وجرائمه/

7 يُنظر، أمبر رحمان، " دور الذكاء الاصطناعي في حملة الإبادة الجماعية التي يشنها الاحتلال الاسرائيلي ضد الفلسطينيين "، مؤسسة الدراسات الفلسطينية، 16 تشرين الأول/ أكتوبر 2024،https://www.palestine-studies.org/ar/node/1656285

8 نيلس أدلر، "ماذا يعني الجنود الآليون (الإنساليون) الأوكرانيون لمستقبل الحرب؟"، الجزيرة، 1 أيار/ مايو 2026، https://www.aljazeera.com/news/2026/5/1/what-do-ukraines-robot-soldiers-mean-for-the-future-of-warfare.

لبنان. أما باحثات الزمالة المتبقيتان تقدّم وجهات نظر نقدية من الجالية الإيرانية والمغربية، مما يوسع الرقعة الجغرافية والنطاق التحليلي للكتاب.

هذا المنشور هو ثمرة تعاون بين «حملة»- المركز العربي لتطوير الإعلام الاجتماعي ومعهد إبراهيم أبو لُغد للدراسات الدولية في جامعة بيرزيت. لعبت كلتا المؤسستين دورًا رائدًا في دراسة تقاطعات التكنولوجيا والسلطة والحقوق، لا سيما فيما يتعلق بالسياق الفلسطيني. وقد استضاف معهد إبراهيم أبو لُغد للدراسات الدولية في جامعة بيرزيت مؤخرًا مؤتمرين دوليين تناولا موضوع عسكرة العالم المُعاصر، وشملا نقاشات وجلسات عن الذكاء الاصطناعي، تكنولوجيا التجسس، ومسارات تعزيز التضامن العابر للحدود.

وبالمثل، أجرت «حملة» في السنين الماضية، أبحاثًا، حملات مناصرة دولية، قامت بتوثيق ورصد ذي علاقة بالحقوق الرقمية الفلسطينية والدور المتنامي للتكنولوجيا في أنظمة الهيمنة والعنف. وشمل هذا العمل، تحقيقات في التجسس الرقمي وقمع الخطاب الفلسطيني على الإنترنت، وتكنولوجيا التجسس وبرامج التجسس والمراقبة، حوكمة المنصات بنهج تمييزي، انقطاع الاتصالات السلكية واللاسلكية في غزة، المخاوف من استخراج البيانات والخصوصية، الحرب المدعومة بالذكاء الاصطناعي، ودور شركات التكنولوجيا الكبرى في إتاحة انتهاكات حقوق الشعب الفلسطيني.

سعت «حملة» إلى وضع التجارب الفلسطينية كمحور لفهم ميول الاستبداد الرقمي العالمية والتقنيات العسكرية وسلطة المنصات. هذا يشمل تقرير «حملة» الأخير، «التربّح من الاحتلال: كيف تمكّن ميتا ماليًا أنشطة الاستيطان والخطاب العنيف ضد الفلسطينيين».[9] يستكشف هذا البحث كيف تسمح «ميتا» لصفحات اليمين الإسرائيلي والحسابات التابعة للمستوطنين بتوليد الإيرادات على الرغم من الترويج للخطاب العنيف والتوسع الاستيطاني والاعتداءات على الفلسطينيين في الضفة الغربية. كما درست أبحاث أخرى لمركز «حملة»، نشر أنظمة الاستهداف القائمة على الذكاء الاصطناعي في غزة، دور البُنى التحتية للحوسبة السحابية في دعم الأنظمة العسكرية الإسرائيلية، الاستخدام المتزايد للتكنولوجيا الرقمية بهدف تجزيء، رصد، والسيطرة على الحياة الفلسطينية السياسية والاجتماعية.[10]

في هذا السياق الأوسع، تتناول الأوراق الخمس في هذا الكتاب مجموعة من الموضوعات المتعلقة بتسليح عمالقة التكنولوجيا وتأثيرهم، الذكاء الاصطناعي، واستخراج البيانات كآليات للتجسس والسيطرة التي يمتد تأثيرها إلى ما هو أبعد من الحيّز التكنولوجيّ. كما تسلط الضوء على الطرق التي تنتشر بها التقنيات القائمة على الذكاء الاصطناعي بحيث تشكل جزءًا من اقتصاد جيو- سياسي أوسع للسيطرة يعمد إلى صياغة شكل تداولها، تنقلها، وتدويلها.

تتبع الورقة الأولى في هذا الكتاب، «السياسة الصناعية ذات الطابع العسكري وشركات التجسس الإسرائيلية»، من تأليف إسلام الخطيب صعود النظام الإسرائيلي كقوة سيبرانية عالمية، وتسلط الضوء على النظام الإيكولوجي المتكامل بين القطاعين

9 أحمد قاضي، "التربّح من الاحتلال: كيف تمكّن ميتا ماليًا أنشطة الاستيطان والخطاب العنيف ضد الفلسطينيين،" حملة- المركز العربي لتطوير الإعلام الاجتماعي، 2026)، https://7amleh.org/post/meta-monetizes-settlements-and-violence-ar

10 حملة – المركز العربي لتطوير الاعلام الاجتماعي، "الحقوق الرقمية الفلسطينية، الإبادة الجماعية، ومسؤولية شركات التكنولوجيا الكبرى "، أيلول/ سبتمبر 2024، https://7amleh.org/storage/genocide/Arabic%20new.pdf

العام والخاص الذي يربط المؤسسات العسكرية والاستخباراتية بقطاع تكنولوجيا التجسس. كما توّضح الورقة كيف يتم تجريب واختبار هذه التكنولوجيا على الفلسطينيين قبل ضبطها لأجل التصدير عالميًا، مع تسليط الضوء على جانب هذه التقنيات العابر للحدود وتداولها.

تناقش الورقة الثانية، «من الاستعمار الاستيطاني والاحتلال بالتحكّم عن بُعد: الابتكار التكنولوجي، والصهيونية النيوليبرالية، والصمود الرقمي في زمن الإبادة الجماعية»، من تأليف أريس بشارة، كيف أدى التقارب بين الابتكار التكنولوجي والاستراتيجية العسكرية إلى إعادة صياغة الاحتلال الإسرائيلي إلى شكل من أشكال الاستعمار الاستيطاني الرقمي، لا سيما بعد السابع من تشرين الأول 2023. تجادل الورقة بأن اقتصاد الابتكار الإسرائيلي يعمل في آن واحد بوصفه مشروعًا وطنيًا ونموذجًا تجاريًا عالميًا، بما يُدرج قطاع التكنولوجيا في أنظمة العنف المستمرة.

أما الورقة الثالثة، «أصوات أسيرة: التجسس الصوتي الخوارزمي في فلسطين»، من تأليف سارة فتح الله، فهي تحلل كيف تم تسليح الصوت في نظام مُتطوّر للغاية من التجسس الجماعيّ، مما يحوّل فعل التحدث إلى فعل أسِر. وتوّضح الورقة كيف يتم اعتراض الأصوات الفلسطينية وتحليلها خوارزميًا ودمجها في أنظمة التحكم التي تتعامل مع التعبير اليومي كدليل أو تبرير مُحتمل. تكشف الورقة عن بنية التجسس الصوتيّ الخوارزمية في فلسطين، وتكشف كيف تحوّل فعل الحديث إلى أداة للهيمنة والرقابة.

وتُعاين الورقة الرابعة، «التضليل الإعلامي وتأثير الدولة عبر إعلانات جوجل»، بقلم ميلودي سيباهبور استخدام إعلانات جوجل كأداة مُرتبطة بالدولة للتأثير المعلوماتيّ، وعمدت إلى تحليل مجموعة من الإعلانات طوال عام كامل تُنسب للحكومة الإسرائيلية. ترى الورقة في مُباحثتها أن منصة إعلانات جوجل تعمل كبنية تحتية قوية للاتصال الاستراتيجي، وتُمكّن الجهات الفاعلة الحكومية من إدراج السرديات التي تُفضلها في لحظات يبحث فيها المستخدمون بشكل نشط عن معلومات، وكيف أنها ساعدت آلة الدعاية (البروباغندا) التابعة للحكومة الإسرائيلية.

أخيرًا، تستكشف ورقة روان يوسف، «الذكاء الاصطناعي في النظام الإنساني في غزة» توظيف الذكاء الاصطناعي والأنظمة الرقمية في العمل الإنساني في غزة في ظل ظروف الحصار، تدمير البنية التحتية، التجسس، والسيطرة الخارجية. تُعاين الورقة كيف يواجه العاملون في الإغاثة والعمل الإنساني هذه الأنظمة ويتعاملون معها ويتنقلون بينها أثناء أعمالهم اليومية، مما يدل على أن الذكاء الاصطناعي يظهر في شكلين مترابطين. الأول في استخدام الموظفين غير الرسمي للأدوات التوليدية من أجل التعامل مع الضغط الإداري؛ والآخر، في الأنظمة المؤسساتية التي تنظم عمليات التسجيل، التحقق، الاستحقاق، الإبلاغ، وتداول البيانات الإنسانية.

مُجتمعة، تُسلّط المساهمات الواردة في هذا الكتاب الضوء على الحاجة المُلحة لتحليل دور الذكاء الاصطناعي وشركات التكنولوجيا في تغيير الواقع السياسي والاجتماعي، واستحداث أساليب الإكراه والعنف في جميع أنحاء العالم. نتمنى أن تُشكّل هذه المساهمات إضافة نوعية إلى تحليل واقع استخدام الذكاء الاصطناعي ودور شركات التكنولوجيا في عالم اليوم. كما نتوجّه بالشكر إلى كل من أسهم في إعداد هذا الكتاب، ونعتذر عن أي سهو أو خطأ مطبعي أو لغوي قد يرد فيه. ونوّد

التنويه إلى أن جميع الأوراق البحثية الواردة فيه قد تُرجمت من اللغة الانكليزية. ويمكن للمهتمين الاطلاع على النسخة الإلكترونية من الكتاب باللغة الإنكليزية عبر موقعي «حملة» - المركز العربي لتطوير الإعلام المجتمعي ومعهد إبراهيم أبو لغد للدراسات الدولية في جامعة بيرزيت.

جلال أبو خاطر و باسل فراج

باسل فرّاج هو مدير معهد إبراهيم أبو لغد للدراسات الدولية وعضو هيئة تدريس في الفلسفة والدراسات الثقافية في جامعة بيرزيت. يركز بحثه على الأسرى السياسيين، والعنف السجني، وممارسات مقاومة الأسرى داخل أنظمة الاعتقال. كما يتناول عمله دراسة تداول الممارسات والسياسات عبر أنظمة الاحتجاز والسجون المختلفة.

جلال أبو خاطر هو مدير السياسات في حملة – المركز العربي لتطوير الإعلام الاجتماعي. يركز عمله على حقوق الفلسطينيين الرقمية، والتكنولوجيا وحقوق الإنسان، ومساءلة الشركات، والمراقبة، والذكاء الاصطناعي، والتقاطعات بين البنى التحتية الرقمية وأنظمة الهيمنة والعنف.

الإرشاد الأكاديمي

تولى إمطانس شحادة منصب المرشد الأكاديمي للفوج الأول من برنامج زمالة مريم أبو دقّة، مرافقاً الزملاء خلال مراحل البحث والإعداد.

إمطانس شحادة هو باحث فلسطيني متخصص في الاقتصاد السياسي والسلوك السياسي وعلاقة الاقتصاد بالمجتمع في البلاد. حاصل على الدكتوراه في العلوم السياسية من الجامعة العبرية في القدس، وماجستير من جامعة حيفا. تتركز أبحاثه على السياسات الاقتصادية والاجتماعية الإسرائيلية، والاقتصاد السياسي المؤثر في المجتمع الفلسطيني، وأثر العولمة على البُنى السياسية والحزبية. يشغل د. شحادة منصب مدير برنامج دراسات إسرائيل في «مدى الكرمل - المركز العربي للدراسات الاجتماعية التطبيقية» في حيفا، ويُدرّس في برنامج الماجستير في الدراسات الإسرائيلية بجامعة بيرزيت.

السياسة الصناعية ذات الطابع العسكري وشركات المراقبة الإسرائيلية

إسلام الخطيب

إسلام مرشحة دكتوراه في مناهج البحث الاجتماعي في كلية لندن للاقتصاد والعلوم السياسية. وُلدت ونشأت في لبنان، وهي باحثة فلسطينية لاجئة يتركز عملها على إنتاج المعرفة المناهضة للاستعمار. تربط أبحاثها بين المراقبة والبُنى التحتية للتكنولوجيا العالمية ومنظومات الهيمنة.

يبحث مشروع إسلام كيف تُدمَج تقنيات المراقبة الإسرائيلية في سلاسل توريد التكنولوجيا العالمية. ومن خلال خرائط استقصائية، تتبّع كيف يُعاد تسويق أدوات طُوِّرت للاحتلال وتُدمج داخل أنظمة الحوكمة العالمية تحت مسميات «السلامة العامة» أو «الأمن السيبراني».

مقدمة

تنبع مكانة إسرائيل كقوة سيبرانية عالمية من منظومة محكمة الترابط بين القطاعين العام والخاص، تصل المؤسسة العسكرية والاستخباراتية بقطاع متقدم لتكنولوجيا المراقبة. [1] وقد تشكّل هذا النظام البيئي عبر عقود من الهيمنة الاستعمارية الاستيطانية والاحتلال العسكري، بما يتيح التطوير السريع للأدوات الرقمية وصقلها ونشرها، وهي أدوات مصممة للمراقبة والتصنيف والإزالة. [2] وتُختبر هذه التقنيات أولاً على الفلسطينيين، ولا سيما في غزة والضفة الغربية، ثم تُطوَّر لاحقاً لأغراض التصدير. [3] وكما يجادل لوينشتاين في كتابه الصادر عام 2023 حول فلسطين بوصفها مختبراً، فقد تحوّل الاحتلال الإسرائيلي إلى نموذج مربح من رأسمالية المراقبة. وأصبح الفلسطينيون موضوعاً لما بات يُعرَّف على نطاق واسع بأنه أول إبادة جماعية في العالم مدعومة بالذكاء الاصطناعي. [4]

تجاوزت شركات الأمن الإسرائيلية منذ زمن طويل دور تسليح الأنظمة القمعية، إذ غدت مندمجة في مشاريع أمنية نيوليبرالية تجعل من الخبرة ذات الطابع العسكري رأسمالاً متنقلاً، يتداول عبر الأسواق العابرة للحدود بطرق تعيد إنتاج الهيمنة المتمحورة حول الولايات المتحدة وتعززها. [5] وغالباً ما تدخل الشركات الإسرائيلية إلى أسواق يتجنبها موردون آخرون. [6] ففي أنحاء أمريكا اللاتينية وأفريقيا وآسيا، رسخت إسرائيل مكانة استراتيجية خاصة من خلال تزويد الدول بحزم متكاملة من البنى التحتية العسكرية والرقمية للمراقبة. [7] وقد وفّرت الأراضي الفلسطينية المحتلة واجهة العرض لهذا النموذج: فتقنيات السيطرة على السكان التي صُقلت في القدس الشرقية [8] والضفة الغربية [9] وغزة، [10] من المراقبة البيومترية المستمرة، إلى الشرطة التنبؤية، والجدران عالية التقنية والطائرات المسيّرة، يُعاد تغليفها للتصدير بوصفها منتجات لـ»الأمن الداخلي». [11] وبالفعل، بحلول منتصف العقد الثاني من

1 Privacy International, “Big Tech’s Bind with Military and Intelligence Agencies,” Privacy International, October 1, 2025, https://privacyinternational.org/long-read/5683/big-techs-bind-military-and-intelligence-agencies.

2 Ihab Maharmeh, “AI as a Tool for Settler-Colonial Projects: How Israel Employs AI to Intensify Colonial Dominance under the Pretext of Counterterrorism,” Critical Studies on Terrorism (2025): 1–24, https://doi.org/10.1080/17539153.2025.2603049

3 Antony Loewenstein, The Palestine Laboratory: How Israel Exports the Technology of Occupation around the World (London: Verso Books, 2023).

4 Amber Rahman, “Explainer: The Role of AI in Israel’s Genocidal Campaign against Palestinians,” Institute for Palestine Studies, 2019, https://www.palestine-studies.org/en/node/1656285.

5 Shir Hever, The Privatization of Israeli Security (London: Pluto Press, 2018).

6 Justice For Myanmar, “Israel’s CAA Industries Ltd Suspected to Have Aided and Abetted the Myanmar Military’s War Crimes and Crimes against Humanity,” June 8, 2023, https://www.justiceformyanmar.org/stories/israels-caa-industries-ltd-suspected-to-have-aided-and-abetted-the-myanmar-militarys-war-crimes-and-crimes-against-humanity

7 Who Profits, “Repression & Diplomacy,” Who Profits Research Center, 2022, https://www.whoprofits.org/publications/report/52?repression-diplomacy

8 Sophia Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights (7amleh – The Arab Center for Social Media Advancement, Summer and Fall 2021), https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pd

9 Amnesty International, “Ban the Scan,” https://banthescan.amnesty.org/opt/

10 Business & Human Rights Resource Centre, “Palantir Allegedly Enables Israel’s AI Targeting amid Israel’s War in Gaza, Raising Concerns over War Crimes,” Business & Human Rights Resource Centre, https://www.business-humanrights.org/en/latest-news/palantir-allegedly-enables-israels-ai-targeting-amid-israels-war-in-gaza-raising-concerns-over-war-crimes/.

11 Rohan Talbot, “Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory,” International Review of the Red Cross 102, no. 914 (2020): 823–49, https://doi.org/10.1017/s1816383121000746.

القرن الحادي والعشرين، باتت إسرائيل تُعرف بأنها «عاصمة الأمن الداخلي»[12] العالمية، إذ تضم أكبر عدد من شركات تكنولوجيا المراقبة للفرد في العالم. [13]

والأهم من ذلك أن وزارة الدفاع الإسرائيلية تضطلع بدور فاعل في تشكيل هذا النظام البيئي. فمن خلال مديرية البحث والتطوير التابعة لها، المعروفة باسم «مافات» (MAFAT)، تربط وزارة الدفاع الطلب العسكري بالابتكار القائم على الشركات الناشئة، ومحوّلةً الاحتياجات العملياتية إلى مسارات تطوير تكنولوجي. [14] وبوصفها واجهة مشتركة بين الوزارة والجهاز التكنولوجي التابع للجيش الإسرائيلي، تنسّق «مافات» بين كبرى شركات الدفاع، بما في ذلك صناعات الفضاء الإسرائيلية ورافائيل وإلبيت سيستمز، مع دمج الجامعات والجهات الفاعلة في القطاع الخاص ضمن شبكة إنتاج موحّدة. [15]

وبحلول عام 2025، وصل هذا التآزر بين القطاعين العام والخاص مستويات غير مسبوقة، إذ جرى دمج أكثر من 130 شركة ناشئة إسرائيلية مباشرة في عمليات الجيش بعد بدء الحرب على غزة عام 2023،[16] تركّز كثير منها على الذكاء الاصطناعي، والأنظمة الذاتية، وأنظمة الاستشعار. وقد جذبت الشركات الناشئة في مجال التكنولوجيا الدفاعية العاملة مع «مافات» تمويلاً تجاوز مليار دولار أمريكي، أي أكثر مما جذبته في جميع السنوات السابقة مجتمعة. [17] ومع بلوغ الإنفاق العسكري العالمي 2. 7 تريليون دولار، يجري استيعاب التقنيات الدفاعية الإسرائيلية بصورة متزايدة في الأسواق العالمية باعتبارها استثمارات عالية العائد. [18] ومن ثم، تصبح الحرب مجالاً مستقراً للتراكم. [19]

وتعمل حالياً في إسرائيل أكثر من ثلاثين شركة مراقبة، أسّس العديد منها أو يعمل فيها قدامى وحدة 8200، وهي وحدة استخبارات إشارات تتمحور مهمتها حول اعتراض الاتصالات الإلكترونية وتحليل البنى التحتية الرقمية. [20] وتندمج هذه الشركات بعمق في البنى التحتية للبيانات العسكرية، ومتوافقة مع أولويات الدولة، مشكلةً ما تصفه صوفيا غودفريند بأنه «مجمع استخباراتي–صناعي».[21]

وفي إطار هذا التشكيل، تعتمد أنظمة الذكاء الاصطناعي مثل «لافندر» و»غوسبل»

12 Neve Gordon, “Israel’s Emergence as a Homeland Security Capital,” in Surveillance and Control in Israel/Palestine: Population, Territory and Power, ed. Elia Zureik, David Lyon, and Yasmeen Abu-Laban (London: Routledge, 2010), 18.

13 Visualizing Palestine, “Fact Sheet: The Israeli Cyber Industry,” Medium, August 30, 2022, https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094

14 Dean Shmuel Elmas, “Defense Ministry Orders Boost Israeli Startups,” Globes, January 21, 2026, https://en.globes.co.il/en/article-defense-ministry-orders-boost-israeli-startups-1001532687

15 Al-Shabaka: The Palestinian Policy Network, “Insulation Not Isolation: Israel’s Super-Sparta War Economy,” 2026, https://al-shabaka.org/briefs/insulation-not-isolation-israels-super-sparta-war-economy/

16 Dean Shmuel Elmas, “Israeli Defense Tech Startups Attract over $1b in Investment,” Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

17 Dean Shmuel Elmas, “Israeli Defense Tech Startups Attract over $1b in Investment,” Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

18 Lisya Bahar Manoah, “Rising Defense Spending: Fueling a Deep Tech Boom in 2026,” Forbes, March 3, 2026, https://www.forbes.com/councils/forbesfinancecouncil/2026/03/03/rising-defense-spending-fueling-a-deep-tech-boom-in-2026/

19 Michael Kwet, “Digital Colonialism: The Evolution of US Empire,” TNI Longreads, March 4, 2021, https://longreads.tni.org/fr/digital-colonialism-the-evolution-of-us-empire.html

20 7amleh – The Arab Center for the Advancement of Social Media, Israel’s Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide (December 2023), https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf.

21 Sophia Goodfriend, “Militarised AI,” London Review of Books (blog), January 28, 2025, https://www.lrb.co.uk/blog/2025/january/militarised-ai.

و»ويرز دادي» على مجموعات واسعة من بيانات المراقبة لإنتاج قوائم استهداف آلية، فيختصر ذلك الفاصل الزمني بين استخراج البيانات والفعل القاتل، ومن ثم يسرّع وتيرة الغارات الجوية ونطاقها. وكما تقول غودفريند، فإن ذلك يُتاح بفعل تزايد عدم التمييز بين شركات التكنولوجيا ووكالات الاستخبارات. فقد جرى تعبئة جنود احتياط من شركات كبرى، بما في ذلك غوغل ومايكروسوفت وأمازون، في العمليات العسكرية، في الوقت نفسه الذي سهّلوا فيه الوصول إلى البنى التحتية التي يساهمون في بنائها في القطاع الخاص. [22] وهكذا تُدمج منصات الحوسبة السحابية، ونماذج الذكاء الاصطناعي، وأنظمة تخزين البيانات واسعة النطاق مباشرة في سير العمل العسكري، حيث تعالج كميات هائلة من المعلومات لتوجيه قرارات الاستهداف. [23] ولا تتمثل النتيجة في مجرد تقارب بين المجالين المؤسسي والعسكري، بل في انهيار أكثر خطورة: أي تحويل جمع البيانات على نطاق واسع إلى مجال متّسع، لا ينتهي، ودائم الإنتاج للأهداف، بما يكثّف نطاق العنف وإيقاعه.

تنعكس الديناميات المبيّنة أعلاه في ممارسات شركات المراقبة نفسها، التي غالباً ما تعتمد عملياتها على بُنى تحتية غامضة وملتبسة قانونياً، لا ينكشف كثير منها إلا من خلال الصحافة الاستقصائية أو الطعون القانونية. وتعمل هذه الشركات ضمن نظام عابر للحدود آخذ في الاتساع، بما يجعل استخراج البيانات على نطاق واسع أكثر انتشاراً وأقل تقيداً بالحدود الإقليمية. وتجسّد شركات مثل مجموعة 9500، التي يقودها ضباط سابقون في الاستخبارات الإسرائيلية والممثَّلة في Cybersec Asia 2026 [24]، وهو منتدى إقليمي رئيسي للأمن السيبراني يجمع الحكومات وشركات التكنولوجيا والجهات الأمنية الفاعلة في منطقة آسيا والمحيط الهادئ، كيفية توسيع شركات المراقبة نطاق حضورها عبر الشبكات العابرة للحدود، وتتوافق مع أجندات جيوسياسية أوسع.

واستناداً إلى بيانات من Start-Up Nation Central، إلى جانب تحليل أطر التصدير التابعة لوزارة الدفاع، وقنوات الشراء، والإفصاحات المؤسسية، تحدد هذه الورقة مجموعة مركّزة من الفاعلين العاملين في المجالات المتقاطعة لتقنيات المراقبة والأمن. ولا تستند الورقة إلى مجموعة بيانات واحدة، بل تعتمد على مقارنة وتحديد مصادر متعددة لرسم خريطة لكيفية عمل هذه الكيانات ضمن بُنى اقتصادية وأمنية أوسع. وعلى الرغم من أن هؤلاء الفاعلين يوصفون غالباً بأنهم «شركات ناشئة»، فإن فهمهم على نحو أدق يكون بوصفهم شركات بالمعنى الاقتصادي. فالشركات التجارية الكبرى المسجلة تشير إلى كيان قانوني يمتلك أصولاً ويدخل في عقود، في حين تشير الشركة بالمعنى الاقتصادي إلى التنظيم الكامن للإنتاج، أي تنسيق رأس المال والعمل والتكنولوجيا عبر شبكة من العلاقات التعاقدية[25]. ويُعد هذا التمييز محورياً في التحليل. فمن خلال فحص الشكل القانوني، وهياكل التمويل، والتمثيل الذاتي، وكل ذلك عبر عدسة السياسة الصناعية، تتتبع الورقة البُنى التحتية التي تُفعَّل من خلالها تقنيات المراقبة عبر الحدود.

وتطرح الورقة ثلاث حجج رئيسية. أولاً، تجادل بأن شركات المراقبة مثل «توكا

22 Ibid.

23 Mahmoud Javadi, “Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan,” Contemporary Security Policy 47, no. 2 (2026): 469–506, https://doi.org/10.1080/13523260.2025.2593247

24 Cybersec Asia, “Speakers,” Cybersec Asia, accessed February 1, 2026, https://cybersec-asia.net/cybersec-asia-speakers/.

25 Jesús Alfaro Águila-Real, “Corporations Are Not Firms,” Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms

غروب» و«كورسايت إيه آي» يجب أن تُفهم بوصفها مكونات متكاملة في السياسة الصناعية الإسرائيلية. وتقليدياً، تشير السياسة الصناعية إلى التشكيل الاستراتيجي للقطاعات الاقتصادية من خلال دعم الدولة، بما في ذلك الاستثمار، والشراء، والتنظيم، وتسهيل التصدير. غير أن هذه السياسة، في الحالة الإسرائيلية، منظمة صراحةً حول الأمن والعسكرة.[26] فشركات مثل «توكا» و«كورسايت إيه آي» لا تقدّم نفسها كمزودين مستقلين للخدمات، بل كفاعلين متفرعين ضمن أنظمة بيئية تربط وكالات الدولة، ورأس المال الخاص، والمؤسسات الدولية. ويتيح لها هذا التموقع أن تعمل كوسطاء يترجمون أولويات الدولة إلى تقنيات قابلة للتسويق، مع توسيع نطاق هذه التقنيات عبر الحدود. ومن ثم، فإن فهم هؤلاء الفاعلين بوصفهم شركات بالمعنى الاقتصادي ينقل التركيز التحليلي بعيداً عن الدولة كوحدة مفردة، نحو البُنى التحتية التي تُنتَج من خلالها المراقبة وتُنشر عبر مجالات مثل الحرب، والشرطة، ومراقبة الحدود.[27]

ثانياً، تجادل الورقة بأن هذا التشكيل القائم على الشركات يسهّل توسّع المراقبة إلى ما وراء الحدود الإقليمية، وينتج أشكالاً من السيطرة لا تقتصر على الحدود المادية. وفي حين شددت الأدبيات القائمة على الكيفية التي تطمس بها الشراكات بين القطاعين العام والخاص التمييز بين البنى التحتية المدنية والعسكرية[28]، تقترح هذه الورقة أن السياسة الصناعية الإسرائيلية تعتمد في الوقت نفسه على الإبقاء على قدر من الفصل الخطابي، على مستوى السردية والتوصيف الذاتي. ويتيح هذا الفصل للشركات الوصول إلى أسواق جديدة، ولا سيما حيث تكون العلاقات السياسية أو الاقتصادية المباشرة مع إسرائيل مقيّدة. ومن خلال التداول العالمي لهذه الشركات، تتمدّد البنى التحتية للمراقبة إلى جغرافيات جديدة، بما يتيح أشكالاً من استخراج البيانات شبه غير محدودة. وبهذا المعنى، فإن توسّع تقنيات المراقبة يفضي أيضاً إلى توسّع في منطق الأمن الإسرائيلي، أي ما يمكن فهمه بوصفه «منطقة أمنية» ممتدة، وهي سردية وأداة رئيسية استخدمتها إسرائيل في السنوات الأخيرة، تتجاوز السياقات المحددة إقليمياً.[29] ومن خلال الوصول إلى بُنى البيانات التحتية العابرة للحدود، تسهم هذه الشركات في توسيع النطاق الذي يمكن ضمنه مراقبة السكان، بمن فيهم الفلسطينيون والمتضامنون معهم، واستهدافهم وإخضاعهم للحكم، تحت الخطاب السائد لـ«الأمن»[30].

ثالثاً، تجادل الورقة بأن مؤسسات التنمية والحوكمة متعددة الأطراف تعمل كواجهات محورية في هذه العملية. فعلى سبيل المثال، توضح حالة «توكا»، المدمجة في مبادرات الحوكمة الرقمية المدعومة من البنك الدولي، وحالة «كورسايت إيه آي»، التي تقيم شراكات مع أجهزة الشرطة في أنحاء أوروبا وآسيا، كيف يُعاد تأطير التقنيات المطوَّرة في سياقات الاحتلال العسكري بوصفها أدوات لـ«بناء القدرات»

26 Seher Bulut, “Israel’s Defense Industry Policy: Security-Centered Transformation, Unregulated Armament and Ethics of Accountability,” CENK 1, no. 2 (2025), https://doi.org/10.5281/zenodo.18082695.

27 Milan Babić, Jan Fichtner, and Eelke M. Heemskerk, “States versus Corporations: Rethinking the Power of Business in International Politics,” The International Spectator: Italian Journal of International Affairs 52, no. 4 (2017): 20–43, https://doi.org/10.1080/03932729.2017.1389151.

28 Joseph F. Getzoff, “Start-up Nationalism: The Rationalities of Neoliberal Zionism,” Politics & Political Theory 38, no. 5 (2020), published March 19, 2020.

29 Binoy Kampmark, “De Facto Occupation: Israel’s Security Zone Strategy,” Countercurrents, April 19, 2025, https://countercurrents.org/2025/04/de-facto-occupation-israels-security-zone-strategy

30 Elia Zureik, “Strategies of Surveillance: The Israeli Gaze,” Jerusalem Quarterly, no. 66 (June 2016): 12, https://doi.org/10.70190/jq.i66.p12

و»الحوكمة الرقمية».[31] ومع أن هذه الدينامية موثّقة في الأدبيات القائمة،[32] توسّع هذه الورقة التحليل من خلال إبراز نشوء أسواق جديدة تتشكل حول التداول العالمي لمنطق الأمن الإسرائيلي، وتوسيع نطاق وصوله العملياتي.

ومن خلال التركيز على «توكا غروب» و»كورسايت إيه آي»، لا تنشغل الورقة بمقارنة المنتجات أو الحصص السوقية، بل تفحص كيفية عمل هذه الشركات ضمن هذا التشكيل الأوسع. إذ تجسّد تشابك المجالات التقنية والعسكرية والسياسية الذي يميّز نظام المراقبة المعاصر، مع الحفاظ على مسافة خطابية استراتيجية عن فاعلي الدولة الإسرائيلية، ولكن ليس عن الأهداف الأوسع التي يسعى هؤلاء الفاعلون إلى تحقيقها.

وتنتظم الورقة في خمسة أجزاء. تبدأ بعرض الإطار النظري والمنهجي. ثم تضع «توكا» و»كورسايت إيه آي» ضمن النظام البيئي السيبراني الإسرائيلي القائم على الشراكة بين القطاعين العام والخاص. ويحلل القسم الثالث كيف تقدم هذه الشركات نفسها للحكومات والمستثمرين والجمهور العالمي، وكيف تعكس هذه السرديات السياسة الصناعية الإسرائيلية وتشكلها في آن واحد.

الإطار المفاهيمي

يبلور هذا القسم الإطار المفاهيمي الذي تُفهم من خلاله الحجج الثلاث المركزية للورقة. ولبناء هذا الإطار، يجمع القسم بين أدبيات دراسات المراقبة، والإمبريالية والاستعمار الرقمي/البياني، مع إسناد التحليل أيضاً في الأدبيات المتعلقة بالسياسة الصناعية، وبالشكل التنظيمي للشركة.

تُعرَّف المراقبة في هذه الورقة بوصفها ممارسةً للحَوكمة وقدرةً مسلَّعة في آن واحد[33] ، أي باعتبارها تجميعاً اجتماعياً–تقنياً [34] يضم معاً وكالات الدولة، والأنظمة القانونية، والبنى التحتية، ومجموعات البيانات، ومسارات العمل/العمالة، والتسويق المؤسسي[35] ويتسق هذا التأطير مع الأعمال التجريبية التي توثق كيف تعمل المراقبة في فلسطين عبر بُنى تحتية متراكبة للسيطرة على السكان،[36], كما يساعد الورقة على توظيف هذه الأعمال بصورة صريحة، وكذلك كيف ترتبط الأنظمة

31 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

32 Gavin Sullivan, “Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage,” Journal of Law and Society (March 2022), https://doi.org/10.1111/jols.12352.

33 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

34 Daniel Marciniak, “Infrastructure Shortcuts: The Private Cloud Infrastructure of Data-Driven Policing and Its Political Consequences,” in States of Surveillance: Ethnographies of New Technologies in Policing and Justice, ed. Maya Avis, Daniel Marciniak, and Maria Sapignoli (London: Routledge, 2025).

35 Daniel Marciniak, “Infrastructure Shortcuts: The Private Cloud Infrastructure of Data-Driven Policing and Its Political Consequences,” in States of Surveillance: Ethnographies of New Technologies in Policing and Justice, ed. Maya Avis, Daniel Marciniak, and Maria Sapignoli (London: Routledge, 2025).

36 (Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear (Cambridge: Cambridge University Press, 2015

الخوارزمية/البيومترية بالضرورات السياسية للتوسع الاستيطاني. [37]

وفي هذا السياق، ولا سيما مع التوسع السريع في تقنيات المراقبة المدفوعة بالذكاء الاصطناعي والمشاريع الإمبريالية التوسعية،[38] عادت السياسة الصناعية إلى الظهور بوصفها ركيزة مركزية من ركائز الحوكمة الاقتصادية المعاصرة. فهي لم تعد تقتصر على الأهداف التنموية أو بهدف الحماية، بل باتت موجَّهة على نحو متزايد نحو ضرورات أمنية وأشكال عسكرية من استراتيجية الدولة. [39] وتبيّن الأدبيات الحديثة أن الحكومات تنشر تدخلات منسقة، تتراوح بين الدعم المالي والمشتريات العامة وضوابط التصدير وتمويل البحث والتطوير، داخل أنظمة إنتاج مدمجة عالمياً، حيث يكون النشاط على مستوى الشركات مدمجاً بعمق في سلاسل قيمة عابرة للحدود. [40] وفي هذا السياق، تعمل السياسة الصناعية، حتى في مجال التكنولوجيا وتحديداً الذكاء الاصطناعي، كآلية لتشكيل أنظمة بيئية كاملة للإنتاج والاستثمار والتكنولوجيا المتقدمة الموجَّهة نحو الحرب، في ظل التداخل المتزايد إلى حدّ عدم القدرة على التمييز بين السياسة الاقتصادية والأمن القومي. [41]

وتبني الورقة على هذه الأدبيات من خلال طرح مفهوم السياسة الصناعية ذات الطابع العسكري، بوصفها شكلاً من أشكال السياسة الصناعية تُنظَّم فيه عملية تطوير القطاعات الاقتصادية وبنيتها وتداولها العالمي صراحةً حول الضرورات العسكرية، ومنطق الأمن، والاستراتيجية الجيوسياسية. [42] وفي الحالة الإسرائيلية، لا يمثل ذلك تطوراً حديثاً، بل بنيةً متجذرة تاريخياً. فكما يجادل طارق دعنا، لا يُعد اقتصاد الحرب الإسرائيلي ظاهرة عارضة أو ظرفية، بل هو اقتصاد ممنهج، متجذر في بناء مؤسسات ذات طابع عسكري قبل قيام الدولة، ومُستدام من خلال تكامل وثيق بين البنى التحتية العسكرية والتكنولوجية والاقتصادية. [43] وبهذا المعنى، تصف السياسة الصناعية ذات الطابع العسكري حالة لا تقتصر فيها الأولويات العسكرية على التأثير في التنمية الاقتصادية، بل تقوم بتنظيمها بصورة فاعلة.

ويتطلب اعتماد عدسة السياسة الصناعية فهماً لكيفية تَشكُّل هذه الآلية ذات الطابع العسكري قانونياً ومالياً وخطابياً. [44] لذلك، تعتمد هذه الورقة تمييزاً مفاهيمياً

37 Sarah Fathallah, "Algorithmic Death-World: Artificial Intelligence and the Case of Palestine," Public Humanities 2 (2026): e7, https://doi.org/10.1017/pub.2025.10113.

38 Neema Iyer, Garnett Achieng, Favour Borokini, and Uri Ludger, Automated Imperialism, Expansionist Dreams: Exploring Digital Extractivism in Africa (Kampala: Pollicy, June 2021), https://pollicy.org/wp-content/uploads/2021/10/Automated-Imperialism-Expansionist-Dreams-Exploring-Digital-Extractivism-in-Africa_2-1.pdf

39 Jostein Hauge, "Industrial Policy Returns as a Weapon of National Security," The Global Currents, December 16, 2025, https://www.theglobalcurrents.com/p/industrial-policy-returns-as-a-weapon.

40 Jostein Hauge, Bruno Houtzager, and Alessandro Julian Hörmann, "The New Economic Nationalism: Industrial Policy and National Security in the United States, China, and the European Union," Geoforum 166 (November 2025): 104382, https://doi.org/10.1016/j.geoforum.2025.104382

41 AI Now Institute, AI Nationalism(s): Global Industrial Policy Approaches to AI, March 12, 2024, https://ainowinstitute.org/publications/research/ai-nationalisms-global-industrial-policy-approaches-to-ai

42 Ulises A. Mejias and Nick Couldry, Data Grab: The New Colonialism of Big Tech and How to Fight Back (Chicago: University of Chicago Press, 2024).

43 Tariq Dana, "Merchants of Death: Israel's Permanent War Economy," Security in Context, January 29, 2024, https://www.securityincontext.org/posts/merchants-of-death-israels-permanent-war-economy.

44 Susannah Glickman, "AI and Tech Industrial Policy: From Post-Cold War Post-Industrialism to Post-Neoliberal Re-Industrialization," AI Now Institute, March 12, 2024, https://ainowinstitute.org/publications/ai-and-tech-industrial-policy-from-post-cold-war-post-industrialism-to-post-neoliberal-re-industrialization

دقيقاً بين «firm» و«company» والفئات القانونية ذات الصلة.[45] فبموجب القانون الإسرائيلي، تُعد «الشركة» Company صيغة قانونية محددة تُسجَّل بموجب قانون الشركات، في حين يعمل مصطلح «شركة كبرى» «corporation» على نحو أوسع كمصطلح جامع يقابل المفهوم القانوني لـ«الشخصية الاعتبارية»، أي شخص قانوني قادر على حيازة الحقوق وتحمل الالتزامات.[46] أما «الشركة الناشئة» Startup فليست فئة قانونية، بل وصف لمرحلة في دورة حياة الشركة يُستخدم في أطر الاستثمار والسياسات العامة. والأهم أن «firm» ليست بحد ذاتها كياناً قانونياً، بل تنظيماً اقتصادياً يقوم على تشكيلة من العقود، وعوامل الإنتاج، وعلاقات الحوكمة التي تنسق رأس المال والعمل والتكنولوجيا.

ويكتسب هذا التمييز أهمية تحليلية حاسمة. فوفقاً لمسجّل الشركات، تُسجَّل كيانات مثل «Corsight AI Ltd» التي تأسست عام 2019 و«Cortica Ltd» تي تأسست عام 2007 رسمياً كشركات خاصة، إلا أنها تعمل كشركات تابعة ضمن شركات/تشكيلات اقتصادية أكبر مدمجة في شبكات معقدة من الاستثمار، وحوكمة الأمن، والتعاقد العابر للحدود، بما في ذلك الاتفاقيات العسكرية. ولا يكفي الشكل القانوني وحده لفهم بنيتها[47] ، التي غالباً ما تنطوي على تشكيلات جماعية، وشركات تابعة، وروابط على مستوى مجالس الإدارة مع مستثمرين وشخصيات سابقة من المؤسسة العسكرية أو الاستخباراتية. وبدلاً من ذلك، يتيح مفهوم «firm» إظهار كيفية عمل هؤلاء الفاعلين كعُقد تشغيلية ضمن اقتصاد أوسع ذي طابع عسكري.

ويزداد ذلك وضوحاً عند النظر إلى البيئة التنظيمية التي تعمل ضمنها هذه الشركات. ففي إسرائيل، تخضع الصادرات الدفاعية لتنظيم وكالة مراقبة الصادرات الدفاعية (DECA) بموجب قانون مراقبة الصادرات الدفاعية لعام 2007، الذي يشترط الحصول على تراخيص لتسويق التقنيات ذات الصلة بالدفاع وتصديرها، ويتماشى مع أنظمة دولية مثل ترتيب فاسنار ونظام مراقبة تكنولوجيا القذائف. وإلى جانب ذلك، تشرف وزارة الاقتصاد على صادرات الاستخدام المزدوج، في حين تخضع الصادرات السيبرانية لمتطلبات متزايدة الصرامة تتعلق بالمستخدم النهائي.[48]

وتُظهر التطورات العالمية الأخيرة في ضوابط التجارة، بما فيها التحديثات التي أُدخلت في أواخر عام 2025، أن ضوابط التصدير هذه لم تعد مقتصرة على التنظيم الوطني، بل أصبحت جزءاً من نظام أوسع للحوكمة الاقتصادية الدولية. فباتت الشركات مُطالبةً الالتزام بمعايير امتثال أكثر صرامة عبر الحدود، بما في ذلك فحوصات أكثر تدقيقاً للمستخدم النهائي، وعمليات العناية الواجبة، والتنسيق مع الأطر التنظيمية للدول الحليفة. ويمدّ ذلك نطاق المسؤولية ليشمل سلسلة التوريد بأكملها، بما يعني أن على الشركات أن تأخذ في الاعتبار ليس فقط الجهة التي تبيع لها مباشرة،

45 Jesús Alfaro Águila-Real, “Corporations Are Not Firms,” Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms.

46 Israel Business Connection, “Company Registration,” Israel Business, accessed March 1, 2026, http://www.israelbusiness.org.il/startingyourbusiness/companyregistration.

47 William Hamilton Byrne, Thomas Gammeltoft-Hansen, and Nora Stappert, “Legal Infrastructures: Towards a Conceptual Framework,” German Law Journal 25, no. 8 (2024): 1229–46, https://doi.org/10.1017/glj.2024.78

48 State Comptroller and Ombudsman of Israel, State Comptroller Report 76B (December 2025), https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2025/2025-12/EN/2025.12-76B-203-EN.pdf

بل أيضاً كيفية استخدام التقنيات ونقلها وتداولها بعد المعاملة الأولية. [49]

وفي هذا المشهد التنظيمي المتزايد التعقيد، يكتسب شكل الشركة بالمعنى الاقتصادي أهمية خاصة. فهؤلاء الفاعلون لا تنحصر أعمالهم في بنية مؤسسية أو إقليمية واحدة؛ بل يعملون من خلال ترتيبات تعاقدية متعددة الطبقات، مثل الشركات التابعة، والشراكات، واتفاقيات الترخيص، والمشاريع المشتركة، ونماذج تقديم الخدمات، وهي ترتيبات يمكن إعادة تشكيلها بحسب البيئات التنظيمية. ويتيح ذلك توجيه التقنيات والخبرات والبيانات عبر قنوات قانونية وجغرافية متعددة، حتى في ظل وجود ضوابط على التصدير. وبدلاً من أن تعمل هذه الشركات ككيانات متكاملة رأسياً، فإنها توزّع عملياتها؛ فقد تُطوَّر المكوّنات الحساسة في كيان، وتُحتفظ بها في كيان آخر، وتُنشر عبر شراكات مع أطراف ثالثة. وما يتشكل هنا هو البنية التحتية المادية لسياسة صناعية ذات طابع عسكري، أي نظام تُنشَر فيه أولويات الدولة الأمنية عبر شركات تقوم بتشغيلها وتوسيعها وعولمتها. وفي هذا التشكيل، يصبح شكل الشركة بالمعنى الاقتصادي الآلية التي تُجعل من خلالها الحرب والمراقبة قابلتين للتوسّع وعابرتين للحدود، بما يحوّل ما قد يبدو نشاطاً تجارياً مجزأً إلى بنية تحتية متماسكة للسيطرة. [50]

وتميل الشركات العاملة في قطاعات السيبرانية والدفاع أو القطاعات المتاخمة للدفاع إلى التسجيل كشركات إسرائيلية خاصة محدودة المسؤولية بهدف التوافق مع متطلبات الترخيص، وغالباً ما تُقسّم التقنيات الخاضعة للرقابة إلى شركات تابعة، أي إلى شركات بالمعنى الاقتصادي، من أجل إدارة التعرض التنظيمي، وتصمّم هياكل حوكمة للتخفيف من المخاطر المرتبطة بالإفصاح عن التقنيات الحساسة. [51] ومن ثم، تعمل السياسة الصناعية ذات الطابع العسكري من خلال شكل الشركة ذاته؛ إذ تصبح الشركات أدوات مؤسسية تُطوَّر من خلالها التقنيات العسكرية، وتُختبر، وتُرخَّص، وتُصدَّر. ولذلك، فإن الشركات، وفق التعريفين الخطابي والقانوني معاً، تعمل في الوقت نفسه كفاعلين اقتصاديين، ووسطاء أمنيين، وأدوات للاستراتيجية الجيوسياسية.

المنهجية

تتطلب دراسة الشركات السيبرانية الهجومية العمل عبر تعتيم منظّم. فهؤلاء الفاعلون يعملون عبر أنظمة مراقبة الصادرات، والشراكات المصنفة، واتفاقيات عدم الإفصاح، ولغة مؤسسية منقّحة عمداً تُخفي كلاً من القدرات وحالات الاستخدام. ويظل الوصول المباشر إلى المعلومات محدوداً، إذ إن العقود الرئيسية غير مفصح عنها، والمواصفات التقنية جزئية، وترتيبات الحوكمة غالباً ما تكون مجزأة عبر ولايات قضائية متعددة. ونتيجة لذلك، لا يمكن للتحليل أن يعتمد على مصدر واحد، بل عليه أن يعيد بناء هذه الأنظمة من خلال آثار متناثرة وغير مكتملة.

49 Shibolet & Co., “Developments in Global Trade Controls: October–December 2025,” Shibolet & Co., January 20, 2026, https://www.shibolet.com/en/developments-in-global-trade-controls-october-december-2025.

50 Laleh Khalili, “How Empire Operates: An Interview with Laleh Khalili,” Viewpoint Magazine, February 1, 2018, https://viewpointmag.com/2018/02/01/empire-operates-interview-laleh-khalili.

51 Haim Ravia and Dotan Hammer, “Israel Publishes Draft Bill on National Cyber Protection,” Pearl Cohen, January 28, 2026, https://www.pearlcohen.com/israel-publishes-draft-bill-on-national-cyber-protection/

ولمعالجة هذه القيود، يعتمد هذا البحث مقاربة منهجية متعددة المصادر، تتعامل مع التعتيم ذاته بوصفه شرطاً تحليلياً. ويثبّت البحث نتائجه عبر المقارنة بين المواد المؤسسية، والتقارير الإعلامية، والأطر التنظيمية، والمعرفة المنتَجة من الحركات، لرسم خريطة لكيفية عمل هذه الشركات وكيفية تمثيلها لذاتها. ويشمل ذلك فحص السِيَر الذاتية للمؤسسين، وشبكات رأس المال المغامر، والإيداعات المؤسسية، حيثما توفرت، وتراخيص التصدير، والشراكات بين القطاعين العام والخاص؛ كما يحلل التغطية الإعلامية عبر مصادر عربية وإنجليزية وعبرية؛ ومراجعة حوكمة الصادرات الإسرائيلية من خلال مواد صادرة عن «سيبات» وهيئات الدولة ذات الصلة. كما يستند البحث إلى مخرجات موجَّهة إلى الشركات، مثل عروض المستثمرين، ومقاطع الفيديو الترويجية، والعروض المقدَّمة في معارض الأمن، لفهم الكيفية التي تبني بها هذه الشركات سردياتها العامة، إلى جانب التحليلات النقدية التي ينتجها باحثون ومنظمات معنية بالحقوق الرقمية.

منهجياً، يجمع البحث بين التحليل الموضوعاتي وتحليل الخطاب لفحص الكيفية التي تعرض بها شركات مثل «توكا» و«كورسايت» تقنياتها عبر هذه المواد. ويحدّد التحليل الموضوعاتي المصطلحات المتكررة، في حين يضع تحليل الخطاب هذه المصطلحات ضمن أطر أوسع تُخفي أصول التقنيات ووظائفها. وتنقل هذه المقاربة التركيز بعيداً عن أوصاف المنتجات، نحو المنطق السياسي والاقتصادي الذي يشكّل كيفية عمل هذه الأنظمة في سياقات حوكمة مختلفة.

غير أن هذه المنهجية، بدلاً من أن تحاول تجاوز التعتيم، تعمل من خلالها. فالطبيعة الجزئية والوسيطة للبيانات المتاحة لا تُعامل بوصفها قيداً فحسب، بل بوصفها مؤشراً إلى الكيفية التي تعمل بها هذه الشركات.

لماذا توكا وكورسايت؟

يركّز هذا البحث على «توكا غروب» و«كورسايت إيه آي» لأنهما حالتان كاشفتان من الناحية التحليلية. فـ توكا غروب هي شركة استخبارات سيبرانية تزوّد الحكومات بقدرات للوصول إلى البيانات واستخراجها من الأجهزة المتصلة، بحيث يصبح «الوصول» بحد ذاته كأداة من أدوات الحوكمة. أما كورسايت إيه آي، وهي شركة تابعة لـكورتيكا، فتطوّر أنظمة متقدمة للتعرف على الوجوه مصممة للتحديد، والتتبع، والمراقبة الفورية في سياقات الأمن والشرطة. وتوفر هاتان الشركتان نقطتي دخول ملموستين يمكن من خلالهما تتبع العمليات الأوسع لاقتصاد المراقبة. ولذلك فإن اختيارهما منهجي، إذ تتيحان للورقة فحص الكيفية التي تعمل بها السياسة الصناعية ذات الطابع العسكري عملياً، مع إبقاء الانتباه إلى كونهما لا تمثلان سوى جزء من نظام بيئي أوسع يشمل مؤسسات الدولة، والفاعلين الماليين، والبنى التحتية العسكرية، والأسواق العالمية.

كلتا الشركتين فاعلتان من القطاع الخاص تعملان داخل الدولة وتتجاوزانها في الوقت نفسه. فهما مسجّلتان رسمياً كشركتين خاصتين، لكنهما تعملان كشركات بالمعنى الاقتصادي مدمجتين في شبكات عابرة للحدود من الاستثمار، والتنظيم، وحوكمة الأمن. وهما تحوزان تراخيص تصدير، وتشاركان في منتديات أمنية دولية، وتضعان نفسيهما كشريكين في مجالات مثل الحوكمة الرقمية، وإنفاذ القانون، والأدلة الجنائية، ومراقبة الحدود. ويُعد هذا التموقع محورياً لدورهما ضمن السياسة الصناعية ذات الطابع العسكري، حيث تعملان كوسطاء يترجمون أولويات

الدولة الأمنية إلى تقنيات قابلة للتوسّع والتسويق. ويسمح لهما شكلهما التنظيمي كشركات بالمعنى الاقتصادي بالتحرك عبر ولايات قضائية متعددة، إذ تستندان إلى وجود في عدة دول، بما في ذلك الولايات المتحدة. ويتيح لهما ذلك الاندماج في بيئات مؤسسية متنوعة، والوصول إلى أسواق قد تكون مقيّدة سياسياً في ظروف أخرى.

ومن ثم، فإن نمو شركات مثل توكا وكورسايت يُتاح بفعل التوافق بين أولويات الدولة، ورأس المال الاستثماري، والأطر التنظيمية، بما في ذلك ضوابط التصدير وأنظمة الشراء التي تسهّل دمجهما في الأسواق الدولية.

وفي الوقت نفسه، تكشف هاتان الشركتان كيف تعمل المراقبة بوصفها حوكمة وبنية تحتية في آن واحد. فتنشأ تقنياتهما ضمن سياق إدارة السكان الفلسطينيين والسيطرة عليهم، لكنها تُصمَّم منذ البداية لتكون قابلة للتوسّع والنقل. وما يُطوَّر كآلية للسيطرة يُعاد تشكيله في نموذج معمّم للحوكمة. وبهذا المعنى، توسّع شركات مثل توكا وكورسايت منطق المراقبة إلى سياقات جديدة، بما في ذلك، على سبيل المثال لا الحصر، المملكة المتحدة وكينيا، إلى جانب دول أخرى. ولذلك، فإن التركيز على هاتين الشركتين يتيح للورقة تتبع الكيفية التي تُفعَّل بها السياسة الصناعية ذات الطابع العسكري من خلال شكل الشركة بالمعنى الاقتصادي، مبيّناً كيف تُتداول المراقبة بعد ذلك كسلعة عالمية.

توكا

«توكا» شركة إسرائيلية خاصة «تربط بصورة علنية عوالم الهجوم السيبراني، والاستخبارات النشطة، والمراقبة الذكية». ومنذ تأسيسها عام 2018، جرى تَمَوضُعها كمصدّر أمني قريب من الدولة. وتُدرج توكا رسمياً لدى «سيبات»،[52] وهي مديرية التعاون الدفاعي الدولي التابعة لوزارة الدفاع الإسرائيلية، كمصدّر دفاعي رسمي ضمن فئتي «الدفاع السيبراني» و«الاستخبارات السيبرانية»، وذلك بحسب ما تأكد في عام 2025. وبعبارة أخرى، فإن الدولة الإسرائيلية نفسها تعترف بمنتجات توكا بوصفها جزءاً من محفظة صادراتها الدفاعية.

ومنذ البداية، قدّمت توكا نفسها «كمتجر اختراق متكامل يعمل لصالح الحكومات»[53]، بوصفها شركة تصمّم «الصمود السيبراني» الوطنية ثم تزوّد الأدوات اللازمة لاختراق البنى التحتية ذاتها التي تساعد في بنائها ومراقبتها والتلاعب بها. وهي تقع عند تقاطع ثلاثة اقتصادات: المجمع العسكري–الاستخباراتي الإسرائيلي، ورأس المال المغامر الأمريكي، وتمويل التنمية متعدد الأطراف، بما في ذلك البنك الدولي، وبنك التنمية للبلدان الأمريكية، ووكالات الأمم المتحدة. وتعمل هذه الاقتصادات مجتمعةً على تحويل القدرات السيبرانية الهجومية إلى مشاريع «بناء قدرات» قابلة للتصدير في الجنوب العالمي وبين الدول الحليفة للولايات المتحدة.[54]

52 Thomas Brewster, “Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT,” Forbes, July 15, 2018, https://www./forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies

53 Thomas Brewster, “Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT,” Forbes, July 15, 2018, https://www./forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies

54 Charles Rollet, “a16z-Backed Toka Wants to Help US Agencies Hack into Security Cameras and Other IoT Devices,” Yahoo Finance (originally published in TechCrunch), December 6, 2024, https://au.finance.yahoo.com/news/a16z-backed-toka-wants-help-183623502.html

1. النشأة، والملكية، والموقع

يجسّد فريق تأسيس توكا مسار الانتقال بين المؤسسات العسكرية والاستخباراتية الإسرائيلية وصناعة السيبرانية في القطاع الخاص. [55] فقد شارك في تأسيس الشركة عام 2018 كل من رئيس الوزراء السابق ورئيس الأركان السابق للجيش الإسرائيلي إيهود باراك، والعميد احتياط يارون روزن، الرئيس السابق لهيئة السيبرانية في الجيش الإسرائيلي. [56] وترسّخ المسيرة الطويلة لباراك على رأس الجهاز الأمني الإسرائيلي، بما في ذلك إشرافه على الموساد والاستخبارات العسكرية بصفته وزيراً للدفاع، موقع توكا بقوة في مدار العمليات السرية للدولة. أما روزن، فيجلب خبرة مباشرة في تصميم ونشر القدرات السيبرانية الهجومية والدفاعية لصالح الجيش الإسرائيلي. [57]

وينضم إليهما المؤسسان المشاركان ألون كانتور وكفير والدمن، اللذان يمثلان الجانب «المدني» من النظام البيئي الإسرائيلي لتكنولوجيا الأمن، من خلال مسيرات مهنية بُنيت في شركات مثل «تشيك بوينت» و:سيسكو»، وهي شركات متجذرة بدورها في شبكات الوحدة 8200. [58] ويشغل والدمن حالياً منصب الرئيس التنفيذي. أما المهندس الرئيسي لحزمة الاختراق التابعة لتوكا، موتي زالتسمان، فقد جاء من وحدة التكنولوجيا في مكتب نتنياهو، وعمل على تقنيات استخبارات هجومية؛ وكان مرتبطاً عن قرب بمشاريع تكنولوجية هجومية في عهد نتنياهو قبل أن تُنقَّح سيرته الذاتية بهدوء بعد تغطية نقدية. [59] ويشغل شخصية بارزة أخرى، هي نير بيليغ، منصب نائب الرئيس للمشاريع الاستراتيجية، وكان قد ترأس سابقاً البحث والتطوير في وحدة التكنولوجيا النخبوية [60]التابعة للمديرية الوطنية للسيبرانية، وعمل عن كثب مع تال غولدشتاين (وهو أحد المهندسين الرئيسيين لاستراتيجية إسرائيل السيبرانية في المحافل العالمية مثل المنتدى الاقتصادي العالمي). [61]

وتعمّق قيادة توكا المؤسسية ومجلس إدارتها هذه الروابط. ففي حين تراجع باراك عن دور نشط في الفترة ما بين 2020 و2024 تقريباً، ظل شخصية مركزية أولية ورمزاً للتموضع الاستراتيجي للشركة. ويضم مجلس الإدارة روزن نفسه والمستثمر التكنولوجي ليئور سوزان، وهو ضابط سابق في القوات الخاصة الإسرائيلية تحوّل إلى رأسمالي استثماري. [62] وتسلّط تقارير حديثة لـ «فوربس» مزيداً من الضوء

55 Toka, “Company Leadership,” Toka Group (archived December 19, 2021), https://web.archive.org/web/20211219162602/https://www.tokagroup.com/company#leadership (for former governance structure).

56 Yasmin Yablonko, “Ehud Barak-Founded Cybersecurity Co Toka Raises $12.5m,” Globes, July 16, 2018, https://en.globes.co.il/en/article-ehud-barak-founded-cybersecurity-co-toka-raises-125m-1001246322

57 Yonah Jeremy Bob, “Ex-IDF Cyber Intel Official: How to Carry Out a Cyber Offense Attack,” The Jerusalem Post, September 14, 2021, https://www.jpost.com/israel-news/ex-idf-cyber-intel-official-how-to-carry-out-a-cyber-offense-attack-677173

58 Corporate Watch, “Check Point Software: Ex-Israeli Military Spooks Profiting from the Cyber Security Industry,” Corporate Watch, November 25, 2019, https://corporatewatch.org/check-point-software-ex-israeli-military-spooks-profiting-from-the-cyber-security-industry/.

59 Jennifer L. Schenker, “Interview of the Week: Tal Goldstein, World Economic Forum Centre for Cybersecurity,” The Innovator, https://theinnovator.news/interview-of-the-week-tal-goldstein-world-economic-forum-centre-for-cybersecurity/.

60 Toka’s ‘About US’ page.

61 Jennifer L. Schenker, “Interview of the Week: Tal Goldstein, World Economic Forum Centre for Cybersecurity,” The Innovator, https://theinnovator.news/interview-of-the-week-tal-goldstein-world-economic-forum-centre-for-cybersecurity/.

62 Samantha Huang, “He Went From Working on a Banana Farm to Selling His First Company to Cisco in the Span of a Decade: Meet Lior Susan, Founding Partner of Eclipse Ventures,” EVCA, March 1, 2021, https://evca.org/content/he-went-from-working-on-a-banana-farm-to-selling-his-first-company-to-cisco-in-the-span-of-a-decade-meet-lior-susan-founding-partner-of-eclipse-ventures.

على اهتمام باراك المستمر بتعبئة رأس المال لصالح توكا إلى جانب محفظته الأوسع من المشاريع. وقبيل الإطلاق العلني للشركة عام 2018، سعى باراك بنشاط لجذب الاستثمار والدعم الاستراتيجي لـ«توكا»، بما في ذلك التواصل مع أفراد ذوي ثروات كبيرة ولديهم صلات حكومية، مقدّماً الشركة صراحةً على أنها «مبنية للحكومات كعملاء». وعلى الرغم من أن هذه الجهود لم تترجم بالضرورة إلى استثمارات مباشرة، فإنها تؤكد كيف جرى تموضع توكا منذ البداية كمؤسسة موجَّهة نحو الدولة، تحتاج إلى رأس المال والوصول السياسي معاً لكي تتوسع. [63]

وترسم قاعدة المستثمرين خريطة مباشرة للتحالفات التكنولوجية والأمنية الأمريكية–الإسرائيلية. وتُعد «Andreessen Horowitz» المعروفة اختصاراً بـ(a16z) من أبرز الداعمين؛[64] ويشغل مؤسسها المشارك مارك أندريسن عضوية مجلس إدارة «ميتا»، وقد ورد اسمه كمدعى عليه في دعاوى خصوصية تتعلق بعدم امتثال ميتا لأوامر تنظيمية أمريكية، بما يبرز كيف تتشابك توكا مع شركات متهمة أصلاً بانتهاكات واسعة النطاق للبيانات. [65] أما Entrée Capital، المذكورة في قسم «المستثمرين» لدى توكا، فيقودها أفياد إيال وران أخيتوف، وتضيف بُعداً آخر من السلالة الاستخباراتية للإشارات، إذ عمل أخيتوف سابقاً في استخبارات الإشارات المعتمدة على الأقمار الصناعية، وشغل مناصب عليا في «أمدوكس» و«كومفرس»، وهما شركتان ارتبطتا بجدالات تجسسية سابقة استهدفت الاتصالات الأمريكية. [66]

وتشير تقارير سابقة لصحيفة «هآرتس» إلى أن عقود توكا لم تكن مدفوعة بالسوق وحده، بل جرى التخطيط لها ودعمها من خلال لجنة مشتركة بين الوزارات أُنشئت في عهد نتنياهو بهدف «تحقيق إمكانات التنمية الدولية» لصالح شركات السيبرانية الإسرائيلية. وعملياً، يعني ذلك أن توكا تُستخدم كأداة من أدوات السياسة الصناعية والخارجية الإسرائيلية. فإدراجها ضمن «سيبات»، وتوظيفها لقدامى الجيش الإسرائيلي والاستخبارات، وتنسيقها مع وزارة الدفاع، كلها أمور تضع توكا كامتداد مخصخص للجهاز السيبراني الهجومي الإسرائيلي، لا كـ «استشارة سيبرانية» محايدة. [67]

وفي أواخر عام 2025، في ظل قيادة الرئيس التنفيذي غريغ سميث، نقلت الشركة مقرها الرئيسي إلى الولايات المتحدة، مع الإبقاء على شركة تابعة في إسرائيل. ويعكس ذلك مرونة شكل الشركة بالمعنى الاقتصادي، إذ تستطيع توكا إعادة تنظيم نفسها عبر الولايات القضائية بما يتماشى مع البيئات الأمنية والتنظيمية والسياسية الرئيسية. [68]

63 Thomas Brewster, “Epstein Could Have Made $100 Million On A Secret Police Tech Investment,” Forbes, February 10, 2026, https://www.forbes.com/sites/thomasbrewster/2026/02/10/epstein-police-surveillance-investments-with-ehud-barak/

64 Andreessen Horowitz, “Investment List,” a16z, accessed April 1, 2026, https://a16z.com/investment-list/

65 Henry Chandonnet, “Marc Andreessen Says Being Controversial Gives His VC Firm an ‘Incredible Competitive Advantage,’” Business Insider, January 12, 2026, https://www.businessinsider.com/marc-andreessen-controversial-competitive-advantage-venture-capital-2026-1

66 James Bamford, “Shady Companies With Ties to Israel Wiretap the U.S. for the NSA,” Wired, April 3, 2012., https://www.wired.com/2012/04/shady-companies-nsa/

67 Omer Benjakob, “This ‘Dystopian’ Cyber Firm Could Have Saved Mossad Assassins From Exposure,” Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

68 Toka, “Toka Deepens Engagement with U.S. and Allied Government Partners, Names Gregg Smith CEO,” February 26, 2026, https://tokagroup.com/news/toka-deepens-engagement-with-u-s-and-allied-government-partners-names-gregg-smith-ceo

2. من «الاستخبارات القانونية» إلى عسكرة إنترنت الأشياء

تُبنى السردية العامة لتوكا بعناية. فالشركة تزعم أنها «تزوّد أجهزة إنفاذ القانون، والأمن الداخلي، والدفاع، والاستخبارات ببرمجيات ومنصة تساعد على تسريع تحقيقاتها وعملياتها وتبسيطها»[69] ، بحيث تتمكن من «الوصول بصورة قانونية وسريعة وسهلة، إلى المعلومات التي تحتاجها للحفاظ على أمن الناس والأماكن والمجتمعات.» وتركّز موادها التسويقية على مفاهيم مثل «الاختراق الأخلاقي»، و»الاعتراض القانوني»، و»الأدلة الجنائية»، و»حماية البنية التحتية الحيوية»، و»الاستراتيجيات السيبرانية الشاملة»[70]. وتقدّم نفسها كشريك يساعد الحكومات على بناء دفاع سيبراني متكامل، وتأمين المدن الذكية، وتعزيز الصمود الوطني.

ويصف عرضٌ تعريفي للشركة حصل عليه صحفيون من هآرتس شركة «توكا» بأنها تقدم «قدرات كانت سابقاً خارج نطاق الوصول»، من شأنها أن «تحوّل مستشعرات إنترنت الأشياء غير المستغلة إلى مصادر استخباراتية» لتلبية «الاحتياجات الاستخباراتية والعملياتية»[71]. وبلغة الشركة نفسها على موقعها الإلكتروني، تُمكّن توكا عملاءها من:

- اكتشاف كاميرات الأمن والكاميرات الذكية والوصول إليها في «منطقة مستهدفة».
- بث الكاميرات والتحكم بها داخل تلك المنطقة على مدى فترة زمنية.
- استهداف المركبات عبر أنظمة الوسائط المتصلة في السيارات، بما يوفّر «أدلة جنائية واستخبارات خاصة بالسيارات»، بما في ذلك تحديد الموقع الجغرافي للمركبات وحركتها.
- جمع استخبارات بصرية من مقاطع فيديو «مباشرة أو مسجلة».
- تعديل البثين الصوتي والمرئي من أجل «إخفاء الأنشطة في الموقع» أثناء «العمليات السرية».

وتُسوَّق أنظمة توكا بوصفها الأداة التي يمكن لقوة شرطة استخدامها لتتبع «هجوم إرهابي» عن بُعد عبر مدينة ما، من خلال السيطرة على شبكات الكاميرات الحضرية. والبنية التحتية نفسها، بحكم تصميمها، تتيح جمع البيانات البصرية والتلاعب بها بصورة سرية «دون ترك أثر».

وتتمثل الوظيفة الأشد إثارة للقلق في تسويق توكا في القدرة على تعديل أو تزييف أو حذف تسجيلات الفيديو، وكذلك التسجيلات الصوتية، دون ترك أثر جنائي رقمي. ويتيح ذلك للمشغّلين ليس فقط مراقبة مشهد ما، بل محو وجودهم بأثر رجعي، أو فبركة الأدلة، أو حجب عنف الدولة. ويزعزع ذلك فعلياً مفهوم الدليل البصري؛ فإذا أمكن تعديل أي تسجيل من كاميرات المراقبة بصمت، فلن تعود المحاكم ولا الجمهور قادرين على الثقة بما يرونه.

69 'Toka's 'About US page

70 Ibid.

71 Omer Benjakob, "This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure," Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

تقنياً، يستفيد نموذج توكا الهجومي من أسطح هجوم لاسلكية شائعة. فكثير من أجهزة كاميرات المراقبة وإنترنت الأشياء تعتمد على شرائح مشتركة، مثل (البلوتوث والواي فاي)، يتم الحصول عليها من مصنّعين خارجيين؛ ويمكن تكرار استغلال ثغرة تُكتشف في شريحة واحدة عبر علامات تجارية متعددة. [72] ويعني اهتمام توكا باستهداف الأجهزة عبر الواجهات اللاسلكية أنها تستطيع تنفيذ هجمات تكتيكية موضعية عندما يكون المشغّل قريباً مادياً من الشبكة المستهدفة، أو تنفيذ هجمات عن بُعد عبر الإنترنت إذا كانت البنية التحتية مكشوفة. [73]

وخلافاً لـ«بيغاسوس»، الذي يركز على الهواتف، تتجه توكا نحو اختراق البيئة بأكملها. وتؤكد تقارير صادرة عن «تك كرانش»، من بين جهات أخرى، أن توكا لا تفصح عن الثغرات التي تكتشفها للمورّدين، بل تحتفظ بثغرات «اليوم الصفري» باعتبارها أصولاً استراتيجية. وهذا النموذج التجاري يُبقي المستخدمين حول العالم في حالة انكشاف أمني متعمّد، من أجل الحفاظ على قدرة عملاء الدولة على اختراق أجهزتهم. [74]

وتصرّ تصريحات توكا نفسها على أنها لا تخدم إلا الحكومات «الموثوقة»، أي تلك التي تتمتع بسجلات جيدة في «سيادة القانون» والحريات المدنية، وذلك من خلال «عملية مراجعة واعتماد سنوية صارمة» تسترشد بمؤشرات الفساد والحريات المدنية، وتدعمها جهات استشارية خارجية، (من بينها شخصيات قانونية واقتصادية بارزة مثل بيتر شَك [75] ويعقوب فرنكل[76]). وهذه هي صيغة «التنظيم الذاتي» المألوفة التي استخدمتها مجموعة «إن إس أو» في سياق بيغاسوس: وعدٌ بأن برمجيات التجسس القوية لن تُستخدم إلا لأغراض أمنية «مشروعة»[77]. وكما يرد في موقع الشركة وبياناتها الصحفية السابقة، لا يوجد في شيفرة توكا، أو هيكل حوكمتها، أو إطار ترخيصها، ما يقيّد على نحو ذي معنى كيفية استخدام أدواتها عملياً. وفي غياب ضمانات قابلة للإنفاذ، يمكن لتقنياتها أن تُستخدم بالسهولة ذاتها ضد أي شخص.

ومجتمعةً، تكشف ادعاءات توكا وقدراتها عن نمط واضح. فالسردية العامة تتمحور حول الاستخبارات القانونية، ومكافحة الجريمة، وحماية البنية التحتية الحيوية. أما الواقع التقني فهو مجموعة من الأدوات التي تتيح للدول السيطرة بصمت على الآثار البصرية والرقمية للحياة اليومية والتلاعب بها ومحوها. وأفضل فهم لهذه الشركة هو بوصفها مصنّعاً لقوة قابلة للإنكار؛ فهي تمنح الدول القدرة على رؤية المزيد والتدخل دون أن تكون «مرئية».[78]

72 Keumars Afifi-Sabet, “Critical Supply Chain Flaw Exposes IoT Cameras to Cyber Attack,” IT Pro, June 16, 2021, https://www.itpro.com/security/vulnerability/359899/critical-supply-chain-flaw-exposes-iot-cameras-to-cyber-attack.

73 Globes Correspondent, “Israeli Cybersecurity Co Toka Raises $25m,” Globes, October 28, 2020, https://en.globes.co.il/en/article-israeli-cybersecurity-co-toka-raises-25m-1001347405.

74 Charles Rollet, “a16z-backed Toka Wants to Help U.S. Agencies Hack into Security Cameras and Other IoT Devices,” TechCrunch, December 6, 2024, https://techcrunch.com/2024/12/06/a16z-backed-toka-wants-to-help-us-agencies-hack-into-security-cameras-and-other-iot-devices/.

75 “Peter H. Schuck,” The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/peter-h-schuck.

76 “Yaakov Frenkel,” The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/yaakov-frenkel.

77 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, “Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware,” Citizen Lab, June 19, 2017, https://citizenlab.ca/research/reckless-exploit-mexico-nso/.

78 Cormac, Rory, and Richard J. Aldrich. 2018. “Grey Is the New Black: Covert Action and Implausible Deniability.” International Affairs 94 (3): 477–494. https://doi.org/10.1093/ia/iiy067.

وتعزز طريقة تمثيل توكا لذاتها في ساحات التصدير الدفاعي الرسمية هذا التموضع. ففي تقاريرها لعام 2025، تعلن الشركة عن نفسها بوصفها مزوّداً لـ«منصات برمجية هي الأولى من نوعها في مجال الأدلة الجنائية الرقمية والاستخبارات»، مستهدفة صراحةً «الحكومات الموثوقة، وأجهزة إنفاذ القانون، والوكالات الأمنية». وتؤكد موادها «الأدوات القانونية للأدلة الجنائية الرقمية وجمع المعلومات الاستخباراتية»، إلى جانب قدرات تتعلق بـ«الاستخبارات المستهدفة» و«العمليات السرية»، مقدّمةً تقنياتها بوصفها أدوات تتيح تحقيقات أسرع، وقابلة للتوسّع، وذات كفاءة عملياتية.[79]

3. الانتشار العالمي

تصرّ توكا، علناً وفي ردودها على التحقيقات، على أنها لا تعمل إلا مع الولايات المتحدة وحلفائها، في قطاعات تشمل الجيش، والأمن الداخلي، ووكالات الاستخبارات، وإنفاذ القانون، وحماية الحدود، وسلطات المدن الذكية.[80] كما تسوّق خدمات استشارية لفرق الاستجابة لطوارئ الحاسوب الوطنية (CERTs)، ولمشغّلي البنية التحتية الحيوية في القطاع الخاص.[81]

جغرافيا العملاء وقطاعاتهم

إسرائيل

الدولة الإسرائيلية هي العميل الأول والتأسيسي لتوكا. وبحلول عام 2021، أفيد بأنها كانت تملك عقوداً بقيمة عدة ملايين من الدولارات مع وكالات أمنية إسرائيلية. وتُنسَّق منتجاتها مع وزارة الدفاع، كما تُعامل موافقات التصدير الخاصة بها كجزء من نظام أوسع لمراقبة الأسلحة في إسرائيل.[82]

نيجيريا

في عام 2020، اختار البنك الدولي توكا لتقديم المشورة للحكومة النيجيرية بشأن تصميم وتعزيز الصمود السيبراني الوطني. وفي إطار هذا المشروع الممول من البنك الدولي، شاركت توكا في بناء أطر الأمن السيبراني في نيجيريا، وقدراتها التقنية، ومهاراتها، بما في ذلك العمل مع فريق الاستجابة لطوارئ الحاسوب الوطني والشركات الخاصة.[83]

79 Cybertoka Ltd. "First-of-their-kind software platforms for digital forensics and intelligence." Company profile in SIBAT (Israel Ministry of Defense) export materials.

80 Thomas Brewster, "Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," Forbes, July 15, 2018, https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/

81 Whitney Webb, "Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of," MintPress News, July 21, 2021, https://www.mintpressnews.com/meet-toka-the-most-dangerous-israeli-spyware-firm-youve-never-heard-of/278020/.

82 Becky Peterson, "The Founders of a Billion-Dollar Israeli Spyware Startup Accused of Helping Saudi Arabia Attack Dissidents Are Funding a Web of New Companies That Hack into Smart Speakers, Routers, and Other Devices," Business Insider, September 5, 2019, https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8.

83 IsraelDefense, "Israel's Toka Advising Nigeria on Cyber Security," February 24, 2020, https://www.israeldefense.co.il/en/node/42066.

مولدوفا

وفي عام 2020 أيضاً، حصلت توكا على عقد ممول من البنك الدولي في مولدوفا لتحديد فجوات الأمن السيبراني في القطاع العام واقتراح استراتيجية لتحسين الجاهزية. وعلى الرغم من أن مولدوفا دولة صغيرة، فإن هذا الانخراط أظهر كيف يمكن لشركات السيبرانية الإسرائيلية أن تستفيد من التمويل متعدد الأطراف للدخول إلى بُنى الدولة التحتية في أوروبا الشرقية. [84]

تشيلي

في عام 2020، اختارت الحكومة التشيلية وبنك التنمية للبلدان الأمريكية توكا لتقديم المشورة بشأن الجاهزية الوطنية للأمن السيبراني وبناء القدرات العملياتية. وتستضيف تشيلي واحدة من أكبر الجاليات الفلسطينية في العالم، وتتمتع بدعم داخلي قوي لفلسطين؛ ولذلك فإن إدخال توكا في الجهاز الأمني التشيلي يحمل دلالة جيوسياسية واضحة بالنسبة إلى إسرائيل. [85]

غانا

كما حصلت توكا على عقد مع البنك الدولي في غانا ضمن برنامج عالمي مماثل لبناء قدرات الأمن السيبراني، موسّعةً بذلك انتشارها في غرب أفريقيا. [86]

المكسيك

تشير بيانات الحكومة المكسيكية إلى أن توكا تعمل بالفعل في المكسيك. وتلاحظ وسائل إعلام إسرائيلية تزايد الاهتمام التجاري الإسرائيلي بالمكسيك في ظل الإدارة الحالية، بما يشير إلى كيفية ربط العقود السيبرانية بتدفقات استثمارية أوسع. [87]

وتشير توكا أيضاً إلى أعمال أو تطوير أسواق في الولايات المتحدة، وألمانيا، وأستراليا، وسنغافورة، وبلجيكا.

استراتيجيات الوصول

إلى جانب العقود الرسمية، عملت قيادة توكا بنشاط على توسيع أسواقها. فقد أفادت تقارير بأن يارون روزن انخرط مع مسؤولين مغاربة في جهود لدخول ذلك السوق. [88] كما كان ممثلو الشركة حاضرين بوضوح في فعاليات أمنية وتكنولوجية مثل «ميليبول»، و«ISS World»، و«جيتكس» في دولة الإمارات العربية المتحدة، ومؤتمرات سيبرانية إقليمية أُطّرت بوصفها منتديات للأمن السيبراني بين إسرائيل

84 Toka, "Toka Awarded World Bank-Financed Contract to Strengthen Moldova's National Cybersecurity Readiness," Yahoo Finance, September 10, 2020, https://finance.yahoo.com/news/toka-awarded-world-bank-financed-100000596.html.

85 Toka, "Toka Selected by Chile and Inter-American Development Bank to Assess and Support Chile's National Cybersecurity Readiness," GlobeNewswire, May 19, 2020, https://www.globenewswire.com/news-release/2020/05/19/2035462/0/en/Toka-Selected-by-Chile-and-Inter-American-Development-Bank-to-Assess-and-Support-Chile-s-National-Cybersecurity-Readiness.html

86 "Toka Scores $25 Million Series B to Enhance Cybersecurity of Gov't Organizations," Israel Defense, October 31, 2020, https://www.israeldefense.co.il/en/node/46195.

87 Jessica Buxbaum, "How Israeli Cyber Weapons Are Taking Over Latin America," MintPress News, March 3, 2023, https://www.mintpressnews.com/israeli-cyber-weapons-taking-latin-america/283926/.

88 Kenza Filali, "L'Israélien Illuminant cherche à investir le marché marocain de la cyberdéfense d'État," Le Desk, July 21, 2023, https://mobile.ledesk.ma/enoff/lisraelien-illuminant-cherche-a-investir-le-marche-marocain-de-la-cyberdefense-detat/.

والإمارات وأوروبا الشرقية.[89] وقد أشارت قيادة المبيعات في توكا علناً إلى نشاط في دولة الإمارات وآسيا، بما يتماشى مع اندفاعة إسرائيلية أوسع نحو أسواق السيبرانية في الخليج وآسيا بعد اتفاقيات التطبيع.

ويُعد الانتشار العالمي لتوكا جزءاً من مشروع سياسي أكبر. فقد حددت إسرائيل صراحةً السيبرانية الهجومية بوصفها ركناً من أركان سياستها الصناعية والخارجية.[90] وعلى الصعيد المحلي، تدعم أدوات توكا توسّع المراقبة وتآكل المساءلة. فهي تمكّن السلطات من تحويل المستشعرات الحضرية المنتشرة في كل مكان إلى أنظمة استخبارات مركزية، ومن تتبع المعارضين وترهيبهم، ومن محو السجلات البصرية لعنف الدولة أو فبركتها. أما دولياً، فيمكن استخدام الأدوات نفسها لمراقبة الحركات العابرة للحدود، بما في ذلك شبكات التضامن، واللاجئون، والناشطون. ويكتسب ذلك أهمية خاصة في ضوء التقارير التي تفيد بأن إسرائيل وشركات حليفة لها استخدمت السيبرانية الهجومية لتتبع حركات مثل حركة المقاطعة وسحب الاستثمارات وفرض العقوبات (BDS) وتعطيلها.

وأخيراً، تسهم توكا في تطبيع السيبرانية الهجومية بوصفها شكلاً من أشكال «التنمية». فعندما تُموَّل حِزم اختراق الكاميرات وأدوات محو الأدلة من قبل البنك الدولي أو بنك التنمية للبلدان الأمريكية تحت عنوان «بناء القدرات السيبرانية»، يكون هناك تحوّل سياسي جارٍ، أي أن المراقبة ذات الطابع العسكري تصبح جزءاً من الأدوات القياسية للحوكمة الحديثة. إن تركيز الغضب الموجه إلى «بيغاسوس» يحجب الانتباه على شركات مثل توكا، التي تتوافق أنشطتها بصورة أكثر راحة مع أجندات الأمن الغربية ومتعددة الأطراف، ومن ثم تجذب قدراً أقل من التدقيق. وتتمثل النتيجة في ترسيخ هادئ لنظام مراقبة عالمي تُدمج فيه التقنيات ذات المنشأ الإسرائيلي بعمق في البنى التحتية الأمنية للدول «الحليفة»، غالباً خارج نطاق الرقابة العامة أو السيطرة الديمقراطية.

كورسايت إيه آي

«كورتيكا» هي شركة إسرائيلية للذكاء الاصطناعي انبثقت عن التخنيون عام 2007.[91] وتقدّم نفسها كقوة مدنية في مجال الذكاء الاصطناعي، تطوّر تعلّماً «مستوحى من الدماغ»، غير خاضع للإشراف ثم تفصل هذه التكنولوجيا الأساسية إلى شركات متخصصة بحسب القطاعات: أ) «أوتوبرينز» للقيادة الذاتية، والمدعومة من «بي إم دبليو» و«تويوتا»،[92] ب) «سي ترو» للفحص الآلي للأمتعة والأمن،[93] ج)

89 AP News, "Garry Kasparov at IMPROVATE Cybersecurity Conference Is Talking About Chess, IA and The Queen's Gambit," AP News (press release), February 16, 2021, https://apnews.com/press-release/pr-newswire/technology-israel-middle-east-garry-kasparov-government-and-politics-e08751ae82db627107fb60602b63062e.

90 Freilich, Charles D, Matthew S Cohen, and Gabi Siboni. 2023. Israel and the Cyber Threat. Oxford University Press.

91 NoCamels Team, "Israeli Startup Raises $5M For Facial Recognition Tech That Can Identify Masked Faces," NoCamels, April 23, 2020, https://nocamels.com/2020/04/israeli-startup-corsight-facial-recognition-tech-masked/.

92 Meir Orbach, "BMW, Toyota Partner With Computer Vision Company Cortica," Calcalist Tech, September 4, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3769653,00.html.

93 SeeTrue, "SeeTrue AI Screening Solution Becomes the First and Only to Receive ECAC Certification for Automated Prohibited Items Detection (APIDS)," PR Newswire, January 8, 2026, https://www.prnewswire.com/apac/news-releases/seetrue-ai-screening-solution-becomes-the-first-and-only-to-receive-ecac-certification-for-automated-prohibited-items-detection-apids-302655629.html.

«فينتيكا» للتحليلات المالية، ومشاريع التصوير الطبي مثل «كورديغايد»، [94] وأخيراً «كورسايت إيه آي»، التي أُطلقت في أواخر عام 2019 بوصفها ذراع التعرف على الوجوه ضمن هذه المحفظة، أي شركة «استخبارات وجوه» أُنشئت لتسويق قدرات الرؤية الحاسوبية لدى «كورتيكا» في مجال المراقبة.[95]

وكورتيكا شركة مملوكة ملكية خاصة، وقد جمعت أكثر من 70 مليون دولار، وتعمل من تل أبيب وحيفا ونيويورك وجنيف.[96] وعلى الرغم من التطبيقات الأمنية الواضحة لمنتجاتها، فإنها غير مدرجة في «سيبات». ويتيح ذلك لكورتيكا أن تقدّم نفسها كشركة ذكاء اصطناعي مدنية، حتى في الوقت الذي تعمل فيه شركاتها المنبثقة مباشرة مع مستثمرين مرتبطين بالدفاع وأجهزة أمن الدولة. [97] فعلى سبيل المثال، أُنشئت كورسايت كمشروع مشترك بين كورتيكا وصندوق «Awz Ventures» الكندي، الذي يقيم شراكة صريحة مع مديرية البحث والتطوير التابعة لوزارة الدفاع الإسرائيلية، ويقوده مسؤولون سابقون في الموساد والشاباك وأجهزة استخبارات أخرى، مع رئيس الوزراء الكندي السابق ستيفن هاربر كمستشار بارز.[98]

1. النشأة، والكوادر، والموقع

تقع كورسايت إيه آي عند تقاطع الخبرة الاستخباراتية الإسرائيلية، والبحث الأكاديمي، ورأس المال الأمني العابر للحدود. وقد شارك في تأسيسها قادة كورتيكا: الرئيس التنفيذي إيغال رايشلغاوز، والدكتورة كارينا أودينايف، وأستاذ التخنيون جوش زئيفي. ورايشلغاوز وأودينايف من قدامى الوحدات التكنولوجية النخبوية في الجيش الإسرائيلي؛ إذ بدأ رايشلغاوز مسيرته في الوحدة 8200، وهي وحدة استخبارات الإشارات والسيبرانية الإسرائيلية. [98] كما يأتي عدد من مهندسي الأبحاث في كورسايت من الوحدة 8200، حاملين معهم خبرة الدولة في المراقبة، والاعتراض، وتحليل البيانات. ويوفّر العمل الأكاديمي لزئيفي الأساس لخوارزميات كورتيكا الجوهرية، بما يمنحها الشرعية العلمية بوصفها «مستوحاة من الدماغ». [99] وعند إطلاقها، كانت كورسايت فريقاً صغيراً، يضم نحو 15 موظفاً موزعين بين إسرائيل والولايات المتحدة، لكنها استفادت من الملكية الفكرية الواسعة لكورتيكا، والتي تشمل أكثر من 250 براءة اختراع، لتدّعي امتلاك حاجز تقني عميق يصعب تجاوزه. [100]

94 Fintica AI, Ltd., “Fintica AI Completes Financial Market Manipulation Detection Pilot for Israel Securities Authority,” PR Newswire, September 14, 2021, https://www.prnewswire.com/il/news-releases/fintica-ai-completes-financial-market-manipulation-detection-pilot-for-israel-securities-authority-301376523.html.

95 Corsight AI, “Corsight AI Becomes First Facial Recognition Provider to Achieve ISO/IEC 42001 AI Management Certification,” March 25, 2025, https://www.corsight.ai/press/corsight-ai-becomes-first-facial-recognition-provider-to-achieve-iso-iec-42001-ai-management-certification/.

96 Cortica Inc., “Cortica Closes $75 Million in New Funding Round and Acquires Springtide Child Development,” PR Newswire, April 18, 2023, https://www.prnewswire.com/news-releases/cortica-closes-75-million-in-new-funding-round-and-acquires-springtide-child-development-301800688.html

97 Rob Watts, “AI in Policing: Doing More with Less,” Corsight AI Blog, September 3, 2025, https://www.corsight.ai/facial-intelligence-uk-policing/.

98 Simon Speakman Cordall, “UK Police to Use AI Facial Recognition Tech Linked to Israel’s War on Gaza,” Al Jazeera, January 28, 2026, https://www.aljazeera.com/news/2026/1/28/uk-police-to-use-ai-facial-recognition-tech-linked-to-israels-war-on-gaza.

99 James Spiro, “Cortica Announces CORDiguide, Medical Spin-Off,” Calcalist Tech, March 9, 2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3897691,00.html.

100 Corsight AI, “Corsight AI Announces U.S. Expansion Due to Market Demand for Leading AI Facial Recognition Technology,” PR Newswire, March 31, 2022, https://www.prnewswire.com/news-releases/corsight-ai-announces-us-expansion-due-to-market-demand-for-leading-ai-facial-recognition-technology-301514859.html.

وتجعل بنية الحوكمة والاستشارات في الشركة نسبها الأمني واضحاً. فيارون أشكنازي، مؤسس «Awz Ventures»، يشغل مقعداً في مجلس إدارة «كورسايت» بصفته شريكاً مديراً؛ وهو ضابط سابق في الشاباك قضى عقداً في قسم حماية الشخصيات المهمة.[101] أما عضو مجلس الإدارة الآخر، اللواء احتياط غيورا آيلاند، فقد ترأس سابقاً مديرية العمليات في الجيش الإسرائيلي، ثم تولى رئاسة مجلس الأمن القومي الإسرائيلي.[102] وكان رون تيبرغ-شاحار، الذي شغل مبكراً منصب مدير العمليات، ضابطاً في الدفاع السيبراني في الجيش الإسرائيلي.[103] ويُدمج هذا التركيز من الشخصيات العسكرية والاستخباراتية السابقة كورسايت في النظام البيئي الأمني نفسه الذي يحكم الاحتلال والعمليات العسكرية الإقليمية.

وفي الوقت نفسه، جمعت كورسايت طبقة قيادية ذات واجهة دولية مصممة لجعل الشركة مقبولة لدى الجهات التنظيمية في أوروبا وأمريكا الشمالية. فقد عيّنت توني بورتر، المفوض السابق لكاميرات المراقبة في المملكة المتحدة، كبيراً لمسؤولي الخصوصية للإشراف على النشر «الأخلاقي»[104]. ولهذا السبب، تتحدث كورسايت إيه آي، بوصفها شركة بالمعنى الاقتصادي، بلغتين في آن واحد: داخلياً، لغة أمن الدولة والقدرات ذات المستوى العسكري؛ وخارجياً، لغة الأخلاقيات، والامتثال، و«الذكاء الاصطناعي المسؤول».

2. من «استخبارات الوجوه» إلى السيطرة على السكان

تطوّر كورسايت ما تسميه حلول «استخبارات الوجوه»، أي أنظمة التعرف على الوجوه التي تحلل الفيديو المباشر أو المسجل من الكاميرات لتحديد هوية الأفراد بسرعة عالية وفي ظروف غير مثالية. وتستوعب منصتها الرئيسية، «Fortify»، تدفقات الفيديو، وتبني قوالب بيومترية من الوجوه، ثم تطابقها مع قوائم المراقبة لإصدار تنبيهات فورية عندما يظهر شخص محل اهتمام أو عندما يدخل شخص ما إلى منطقة محظورة.[105]

ومن الناحية التقنية، تزعم الشركة أن خوارزمياتها، المستمدة من محرك الذكاء الاصطناعي المستقل التابع لكورتيكا، قادرة على التعرف على الأفراد حتى عندما يكون أقل من نصف الوجه مرئياً، أو عندما يكون الشخص متحركاً، أو محجوباً جزئياً، أو يرتدي قناعاً أو خوذة. وخلال جائحة كوفيد19-، سوّقت كورسايت هذه القدرة بقوة باعتبارها ميزة تميّزها، إذ أعلنت عن القدرة على تحديد هوية الأفراد الذين يرتدون الكمامات بدقة، دعماً لإنفاذ الحجر الصحي، والمساعدة في تتبع المخالطين. وتُباع القدرة نفسها اليوم كميزة في مجالات إنفاذ القانون، ومراقبة الحدود، ونشر أنظمة «المدينة الآمنة»، حيث قد يغطي الناس وجوههم أو تلتقطهم الكاميرات في إضاءة ضعيفة ومن زوايا حادة.[106]

101 Awz Ventures, "The Awz Story," accessed April 1, 2026, https://www.awzventures.com/awz-story/.

102 Maj. Gen. (res.) Giora Eiland, "Author Page," Begin-Sadat Center for Strategic Studies, accessed April 1, 2026, https://besacenter.org/author/geiland/.

103 Ron Tiberg-Shachar," The Org, accessed April 1, 2026, https://theorg.com/org/saiflow/org-chart/ron-tiberg-shachar"

104 Biometrics and Surveillance Camera Commissioner, Biometrics and Surveillance Camera Commissioner's Annual Report 2023 to 2024, December 2, 2024, https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2023-to-2024/biometrics-and-surveillance-camera-commissioners-annual-report-2023-to-2024-accessible

105 Corsight AI, "Fortify," accessed April 1, 2026, https://www.corsight.ai/product-fortify/.

106 Corsight, "Corsight AI Facial Intelligence in Retail," YouTube video, February 14, 2024, https://www.youtube.com/watch?v=GXDjkwWetpg.

وتشير كورسايت إيه آي إلى تقييمات مستقلة، مثل اختبار التعرف على الوجوه الذي أجرته وزارة الأمن الداخلي الأمريكية عام 2020، لإظهار أن نظامها جاء ضمن المراتب العليا من حيث الدقة، بما في ذلك في ظروف ارتداء الكمامات. [107] وتصر كورسايت، من خلال ورقة كتبها توني بورتر نفسه، على أن نماذجها غير متحيزة للعرق، والجندر، والعمر، متناولةً بذلك الأداء التمييزي الموثق جيداً لكثير من أنظمة التعرف على الوجوه. [108]

ومنذ نشأتها، عملت كورسايت إلى جانب الوكالات العسكرية والاستخباراتية الإسرائيلية، التي أصبحت من أوائل الجهات التي تبنّت أنظمتها. وتقر الشركة بأن كثيراً من عمليات النشر هي عمليات سرية تخص «وكالات استخبارات ووحدات خاصة لإنفاذ القانون».[109]

ويُعد أحد أوضح الأمثلة على ذلك الأراضي الفلسطينية المحتلة. فقد أظهرت تقارير منظمة العفو الدولية أن تقنية التعرف على الوجوه التي تطورها كورسايت تُستخدم من قبل الاستخبارات العسكرية الإسرائيلية لبناء قواعد بيانات بيومترية للفلسطينيين والحفاظ عليها. [110] وخلال الحرب على غزة، حمل الجنود كاميرات مزودة ببرمجيات كورسايت عند نقاط التفتيش وعلى مسارات الإخلاء، حيث كانوا يمسحون وجوه الفلسطينيين دون موافقة، ويقارنون تلك الصور بقوائم المراقبة.

أما في الخارج، فإن الغالبية الساحقة من عمليات النشر تتم في مجالات إنفاذ القانون، ومراقبة الحدود، ومراقبة البنية التحتية الحيوية، مثل شبكات كاميرات المراقبة في المدن، والمطارات، والمناجم والبنوك، والمعابر الحدودية، والفعاليات العامة. [111] [112]

وبهذا المعنى، تعمل «كورسايت» كنقطة لقاء في تمديد منطق الأمن الإسرائيلي إلى ما وراء الحدود الإقليمية. فهي توسّع نطاق الممارسات الأمنية الإسرائيلية إلى ولايات قضائية جديدة، وتعيد توزيع القوة لصالح الدول والجهات المؤسسية التي تنشر هذه الأنظمة، في حين تضع الأفراد والمجتمعات في أماكن أخرى كأهداف للمنطق نفسه من المراقبة، والتصنيف، والسيطرة.

3. الانتشار العالمي

يرسم توسّع كورسايت خريطة الطلب العالمي على البنية التحتية للمراقبة، ويعكس استراتيجية إسرائيل الأوسع في تصدير تقنيات الأمن بوصفها شكلاً من أشكال الدبلوماسية، والتنمية، وبناء النفوذ. [112] وتفيد الشركة بأن لديها عمليات

107 Tony Porter, "Facial Recognition Technology: Blasting the Bias Narrative Out of the Water?," Biometric Technology Today 2022, no. 12 (2022), https://doi.org/10.12968/S0969-4765(22)70622-4.

108 Tony Porter, "Facial Recognition Technology: Blasting the Bias Narrative Out of the Water?," Biometric Technology Today 2022, no. 12 (2022), https://doi.org/10.12968/S0969-4765(22)70622-4.

109 Sheera Frenkel, "Report Reveals Google & Corsight Technologies' Role in Israel's Expansive Facial Recognition Program in Gaza," Business & Human Rights Resource Centre, March 27, 2024, https://www.business-humanrights.org/en/latest-news/report-reveals-google-corsights-technologies-role-in-israels-expansive-facial-recognition-program-in-gaza/.

110 Amnesty International, "Israel/OPT: Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid," May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

111 Corsight AI, "Facial Recognition at Airports," accessed April 1, 2026, https://www.corsight.ai/airports/.

112 This is well-highlighted in a paper by Lior Tabansky, "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy," NATO Cooperative Cyber Defence Centre of Excellence, 2018, https://ccdcoe.org/uploads/2018/10/Art-04-Towards-a-Theory-of-Cyber-Power-the-Israeli-Experience-with-Innovation-and-Strategy.pdf.

نشر في أكثر من خمسين دولة، غالباً من خلال مدمجين محليين ومشاريع «المدينة الآمنة» التي تربط بين الإضاءة الذكية، والكاميرات، والتحليلات. [113]

1.3 منطقة جنوب غرب آسيا وشمال أفريقيا

قادت «Awz» التوسع نحو أسواق الخليج التي فتحتها اتفاقيات أبراهام. فقد أنشأت «Awz» شركة تابعة في دولة الإمارات العربية المتحدة لتوجيه تقنيات الأمن الإسرائيلية، بما في ذلك كورسايت، من خلال ابرام عقود إماراتية وإقليمية. [114] وقد أقرّ مسؤولون تنفيذيون في كورسايت بوجود محادثات مع قوات شرطة خليجية، بما يتماشى مع جهود أوسع لوضع إسرائيل كمزوّد رئيسي لمراقبة المدن الذكية والحدود لدول مثل الإمارات العربية المتحدة والمملكة العربية السعودية. [115]

2.3 أفريقيا

في أفريقيا، تدخل كورسايت إلى حد كبير من خلال الشراكات. ففي ناميبيا، أصبحت «Schoemans Technologies» موزعها الحصري، مسوّقةً أنظمة التعرف على الوجوه للحكومة والمؤسسات. [116] وفي جنوب أفريقيا، دمجت شركة الأمن «E-Thele» خوارزميات «كورسايت» في أنظمة مراقبة للمناجم والبنوك، لمراقبة الوصول إلى المواقع ذات القيمة العالية. [117]

3.3 آسيا والمحيط الهادئ

في الفلبين، نشرت مدينة سانتا روزا منصة كورسايت ضمن مبادرة «المدينة الآمنة»، حيث شغّلت عمليات مسح فورية وجنائية رقمية عبر شبكة كاميرات المراقبة التابعة لها لرصد الأشخاص المطلوبين والتعرف على الأفراد المفقودين. [118] كما سعت كورسايت إلى الحصول على فرص في الهند، حيث وقّعت مذكرة تفاهم مع مؤسسة الإلكترونيات التابعة لولاية آسام (AMTRON) لإنشاء مركز تميز للتعرف على الوجوه في غواهاتي لعملاء الحكومة الهندية. [119] وتستهدف شراكة مع الموزع السنغافوري «Netpoleon» أسواق جنوب شرق آسيا على نحو أوسع، من خلال الجمع بين خوارزميات كورسايت والمدمجين الأمنيين المحليين لإدخال التعرف على الوجوه في البنى التحتية للأمن الحضري والوطني. [120]

113 Iain Overton, "Corsight's Crisis: Why British Police Forces Must Rethink Their Israeli Facial Recognition Partners," Action on Armed Violence (AOAV), July 7, 2025, https://aoav.org.uk/2025/corsights-crisis-why-british-police-forces-must-rethink-their-israeli-facial-recognition-partners/.

114 Brigitte Bureau, "Stephen Harper Involved in Company Looking to Arrange Sale of Surveillance Tech to UAE," CBC News, September 29, 2021, https://www.cbc.ca/news/politics/harper-united-arab-emirates-surveillance-technology-1.6192281.

115 "Israelis Pour into UAE for Business and Pleasure," Ynetnews, December 9, 2020, https://www.ynetnews.com/travel/article/Bk00xPYRiD.

116 Corsight AI, "Corsight AI Announces Strategic Partnership With Schoemans Technologies in Namibia," Business Wire, January 30, 2025, https://www.businesswire.com/news/home/20250130146143/en/Corsight-AI-Announces-Strategic-Partnership-With-Schoemans-Technologies-in-Namibia.

117 eThele, "Partners," accessed April 1, 2026, https://www.ethele.co.za/partners/.

118 Corsight AI, "Santa Rosa Safe City Enhances Public Safety with Corsight AI's Unique Facial Intelligence Technology," Business Wire, September 26, 2024, https://www.businesswire.com/news/home/20240926379646/en/Santa-Rosa-Safe-City-Enhances-Public-Safety-with-Corsight-AIs-Unique-Facial-Intelligence-Technology.

119 "Corsight AI Partners for Facial Recognition Projects in India," Biometric Update, August 19, 2021, https://www.biometricupdate.com/202108/corsight-ai-partners-for-facial-recognition-projects-in-india.

120 Corsight AI, "Leading Facial Recognition Technology Provider, Corsight AI, Announces Netpoleon as Distribution Partner for Asia," PR Newswire, May 12, 2021, https://www.netpoleons.com/news/leading-facial-recognition-technology-provider-corsight-ai-announces-netpoleon-as-distribution-partner-for-asia.

3. 4 أوروبا

يكمن حضور كورسايت في أوروبا من خلال المطارات، والمستشفيات، والشرطة. وتفيد الشركة بأن لديها عمليات نشر في عدة مطارات ومرافق رعاية صحية أوروبية ضمن أنظمة التحكم في الوصول والأمن. [121] وفي المملكة المتحدة، اعتمدت شرطة إسيكس نظاماً حياً للتعرف على الوجوه مبنياً على تقنية كورسايت، مستخدمةً كاميرات في الفعاليات العامة ومحطات النقل لمسح الحشود واعتقال المشتبه بهم. وتقدّم قيادة كورسايت في المملكة المتحدة، المؤلفة من شخصيات سابقة في تكنولوجيا الشرطة، هذه العمليات بوصفها ممتثلة تماماً للأنظمة الوطنية، رغم المخاوف المتعلقة بالحريات المدنية. [122]

3. 5 الأمريكتان

تُعد أمريكا اللاتينية من مناطق النمو الرئيسية. ففي البرازيل، عقدت كورسايت شراكات مع شركات مثل «Teltex» و«Segurimax» لنشر مراكز للتعرف على الوجوه عبر كتائب شرطة ولاية ساو باولو. [123] ودمجت شركة الإضاءة الذكية الإسرائيلية «Juganu» نظام كورسايت في أعمدة إنارة «ذكية» على جسر الصداقة بين البرازيل وباراغواي، بحيث تلتقط وجوه المسافرين ولوحات أرقام المركبات وتبث تلك البيانات إلى سلطات الحدود، في مثال على مراقبة بيومترية منسوجة داخل بنية تحتية تبدو محايدة، أي الإضاءة، لكنها تعمل كوحدة لجمع البيانات. [124] وفي باراغواي، رخّصت «Grupo Vázquez» خوارزميات كورسايت لإدماج التعرف على الوجوه عبر أعمالها المتنوعة وبيع الخدمات لوكالات حكومية. [125]

وفي المكسيك، عقدت كورسايت شراكة مع شركة الأمن «ISEG» لتركيب تقنية التعرف على الوجوه في ثلاثة مستشفيات في مونتيري، ضمن شبكة الرعاية الصحية «Auna»، لمراقبة وحدات العناية المركزة وغيرها من المناطق الحساسة. [126] كما ارتبطت كورسايت بالشرطة الفيدرالية المكسيكية ووكالات إقليمية أخرى. [127] وفي كولومبيا، نفذت شرطة بوغوتا الحضرية تجربة عام 2023 باستخدام كورسايت للتعرف على مشتبه بهم من لقطات كاميرات المراقبة. وفي أنحاء الأمريكتين، يتكرر النمط نفسه: الدمج في الشرطة، ومراقبة الحدود، والمستشفيات، والمواقع التجارية عالية القيمة، تحت شعار التحديث والكفاءة . [128]

ويقود توسّع كورسايت استراتيجية إعلانية تجمع بين الاعتمادات الأمنية النخبوية

121 "EU AI Pact Sets New Standards for Ethical AI Use Across Europe," Biometric Update, September 13, 2024, https://www.biometricupdate.com/202409/eu-ai-pact-sets-new-standards-for-ethical-ai-use-across-europe

122 Robert Booth, and Mark Wilding. "Essex Police Pause Facial Recognition Camera Use After Study Finds Racial Bias." The Guardian, March 19, 2026. https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias

123 Corsight AI. "Corsight AI Partners with Segdboa to Provide São Paulo Military Police with Facial Intelligence Capabilities." Business Wire, June 19, 2024. https://www.businesswire.com/news/home/20240619024171/en/Corsight-AI-Partners-with-Segdboa-to-Provide-So-Paulo-Military-Police-with-Facial-Intelligence-Capabilities.

124 Techtime. "Juganu Made the Brazil-Paraguay Border Safer." Techtime, July 2, 2020. https://techtime.news/tag/smart-city/.

125 Business Wire. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Financial Post, September 2, 2024. https://financialpost.com/pmn/business-wire-news-releases-pmn/corsight-ai-partners-with-itti-from-grupo-vazquez-to-enhance-security-efficiency-and-user-experience-with-facial-intelligence.

126 Corsight AI. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Security Journal Americas, September 2024. https://securityjournalamericas.com/partnership-for-facial-intergration/

127 Ibid.

128 IFSEC Insider. "Bogotá Police Using Facial Recognition to Enable Arrest of Murder and Theft Suspects." IFSEC Global, November 8, 2023. https://www.ifsecglobal.com/video-surveillance/bogota-police-using-facial-recognition-to-enable-arrest-of-murder-and-theft-suspects/

والخطاب الأخلاقي. فالشركة تبرز أداءها «بالمستوى العسكري» ونسبها إلى الوحدة 8200 عند البيع للأجهزة الأمنية، بينما تؤكد الأخلاقيات، والامتثال للخصوصية، ووجود منظم بريطاني سابق للمراقبة عند مخاطبة الجمهور والجهات التنظيمية في الديمقراطيات الليبرالية.[129] وعلى الرغم من هذه الروابط المؤسسية العميقة مع الجيش الإسرائيلي، أكد الرئيس التنفيذي لكورسايت علناً أن الشركة «لا تبيع للصين أو روسيا أو ميانمار بسبب حقوق الإنسان والأخلاقيات»، مقدّماً تقنيتها بوصفها «قوة للخير» من أجل إنفاذ القانون.[130] وتضع مثل هذه الادعاءات الشركة ضمن إطار أخلاقي انتقائي، حيث لا تُساءَل شرعية المراقبة في ذاتها، بل يُعاد تأطيرها من خلال اختيار العملاء، بما يسمح بتسويق التكنولوجيا بوصفها مسؤولة وواعية بالحقوق، حتى وهي تظل مدمجة في بُنى تحتية للسيطرة ذات طابع عسكري.

الخلاصات الرئيسة

لا تكمن أهمية هذه النتائج فيما تفعله هذه الشركات فحسب، بل في البنية التحتية التي تجعل عملياتها ممكنة. وتُظهر نتائج هذه الورقة أن توكا وكورسايت إيه آي لا يمكن فهمهما على نحو أدق بوصفهما شركتين تكنولوجيتين خاصتين ومعزولتين، بل بوصفهما أدوات على مستوى الشركة بالمعنى الاقتصادي، تُغسل، بالمعنى الحرفي، من خلالها السياسة الصناعية الإسرائيلية ذات الطابع العسكري.[131] ويتوافق ذلك مع مجموعة متنامية من الأدبيات التي تفهم المراقبة بوصفها ناشئة من تقاطع سلطة الدولة،[132] والفاعلين المؤسسيين،[133] والأسواق العابرة للحدود،[134] لا من مجالات مؤسسية منفصلة.

وعلى الرغم من أن توكا وكورسايت تعملان في مجالين تكنولوجيين مختلفين، فإنهما تؤديان أدواراً متكاملة داخل بنية السياسة الصناعية نفسها. فتجسّد توكا كيفية دمج القدرات السيبرانية الهجومية في الحوكمة من خلال لغة الاستخبارات القانونية والمرونة، في حين تُظهر كورسايت كيفية تطبيع المراقبة البيومترية من خلال خطابات الذكاء الاصطناعي الأخلاقي والامتثال. واستناداً إلى الأعمال الحديثة لمعهد «AI Now» حول «قوميات الذكاء الاصطناعي»، التي تبرز كيف تعبّئ الدول السياسة الصناعية لتشكيل أنظمة الذكاء الاصطناعي بما يتماشى مع الأولويات

129 Liberty. "Liberty Responds to Essex Police Pausing Use of Facial Recognition Cameras Due to Racial Bias." Liberty Human Rights, March 20, 2026. https://www.libertyhumanrights.org.uk/issue/liberty-responds-to-essex-police-pausing-use-of-facial-recognition-cameras-due-to-racial-bias/

130 Cheslow, Daniella. "Israeli Firm Develops Body Cams with Facial Recognition Technology." The Times of Israel, January 23, 2022. Updated January 25, 2022. https://www.timesofisrael.com/israeli-firm-develops-body-cams-with-facial-recognition-technology/.

131 Yaron Salman, "Light unto the Nations Through Arms Sales: Israel's Arms Diplomacy Goals, Achievements, and Limitations," Contemporary Review of the Middle East 12, no. 2 (2025), https://doi.org/10.1177/23477989251318874.

132 Feldstein, Steven. "Front Matter." In The Global Expansion of AI Surveillance. Washington, DC: Carnegie Endowment for International Peace, 2019. http://www.jstor.org/stable/resrep20995.1.

133 7amleh – The Arab Center for the Advancement of Social Media. Israel's Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide. December 2023. https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

134 Ahmad H. Sa'di, "Israel's Settler-Colonialism as a Global Security Paradigm," Race & Class 63, no. 2 (2021): 21–37, https://doi.org/10.1177/0306396821996231.

الجيوسياسية والاقتصادية،[135] يمكن فهم السياسة الصناعية الإسرائيلية للذكاء الاصطناعي كتشكيل مكثّف يُنظَّم فيه تطوير الذكاء الاصطناعي صراحةً حول العسكرة والضرورات الأمنية. [136]

وتُظهر النتائج أيضاً تطبيع المراقبة، وهو ما وصفه بعض الباحثين بأنه خطاب تكنوقراطي. [137] وتستخدم الشركتان مصطلحات السلامة العامة، والصمود السيبراني، والاستخبارات القانونية، والذكاء الاصطناعي الأخلاقي كأطر لإضفاء الشرعية، لا كأوصاف محايدة. وعلى المستوى المادي، تُظهر النتائج أن شكل الشركة بالمعنى الاقتصادي مركزي في عولمة التقنيات ذات الطابع العسكري. [138] فشركات مثل توكا وكورسايت لا تكتفي بتسويق ابتكارات الدولة تجارياً؛ بل تنظّمها، وتتوسطها، وتنشرها عبر ترتيبات تعاقدية وتنظيمية معقدة. ويدعم ذلك ويوسّع الحجج المتعلقة بنشوء «مجمع استخباراتي–صناعي»، تُدمج فيه الفاعلون من الشركات الكبرى بنيوياً في البنى التحتية الأمنية للدولة. [139]

وانسجاماً مع الانتقادات الموجهة إلى «الذكاء الاصطناعي الأخلاقي» بوصفه شكلاً من أشكال الحوكمة بلا قيود،[140] تشير النتائج إلى أن الادعاءات الأخلاقية تعمل كآليات للتمايز السوقي أكثر من كونها قيوداً جوهرية. وأخيراً، تعزز النتائج الانتقادات القديمة لتآكل الحدود بين الدولة والسوق في إنتاج الأمن. [141]

لقد موّل البنك الدولي وبنك التنمية للبلدان الأمريكية، خلال العقد الماضي، برامج للأمن السيبراني والحوكمة الرقمية مكّنت من دمج شركات مراقبة إسرائيلية في بُنى الدولة التحتية عبر الجنوب العالمي وما بعده. وبين عامي 2020 و2023، مُنحت عقود في نيجيريا ومولدوفا وغانا وتشيلي إلى توكا غروب. وبالتوازي مع ذلك، دمجت كورسايت إيه آي أنظمتها في بُنى الشرطة، ومراقبة الحدود، والمراقبة الحضرية في أكثر من خمسين دولة.

أولاً، ليست شركات مثل توكا وكورسايت فاعلين تقليديين من القطاع الخاص يعملون على هوامش الدولة. بل هي امتدادات تنظيمية لسياسة صناعية أوسع ذات طابع عسكري، تترجم القدرات العسكرية والاستخباراتية إلى منتجات قابلة للتوسّع في الأسواق العالمية. وتعمل كورسايت إيه آي وفق منطق موازٍ. فهي تنشأ من شبكة من المهندسين المدرَّبين عسكرياً وهياكل حوكمة مرتبطة بالاستخبارات،

135 Amba Kak, AI Nationalism(s): Global Industrial Policy Approaches to AI—Executive Summary (New York: AI Now Institute, 2024), https://ainowinstitute.org/publications/ai-nationalisms-executive-summary.

136 Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," Journal of Global Security Studies 9, no. 2 (June 2024): ogae009, https://doi.org/10.1093/jogss/ogae009.

137 David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies," in Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, ed. David Lyon (London: Routledge, 2003), 13–30.

138 Rita Abrahamsen and Michael C. Williams, "Securing the City: Private Security Companies and Non-State Authority in Global Governance," International Relations 21, no. 2 (2007): 237–253, https://doi.org/10.1177/0047117807077006.

139 This paper has drawn on and referenced multiple works by Sophia Goodfriend, building on them to develop its argument. See: Sophia Goodfriend, "New Tech, Old War," London Review of Books (blog), July 2023, https://www.lrb.co.uk/blog/2023/july/new-tech-old-war

140 Jacob Metcalf, Emanuel Moss, and danah boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," Social Research: An International Quarterly 82, no. 2 (Summer 2019): 449–476 (New York: Data & Society Research Institute), https://datasociety.net/wp-content/uploads/2019/09/Owning-Ethics-PDF-version-2.pdf.

141 Linda Weiss and Elizabeth Thurbon, "Power Paradox: How the Extension of US Infrastructural Power Abroad Diminishes State Capacity at Home," Review of International Political Economy 25, no. 6 (2018): 779–810, https://doi.org/10.1080/09692290.2018.1486875.

وتطوّر أنظمة تعرف على الوجوه قادرة على تحديد هوية الأفراد في ظروف الحجب، والحركة، وضعف الرؤية.

ثانياً، إن التوسع العالمي لهذه التقنيات يُتاح من خلال شكل الشركة بالمعنى الاقتصادي نفسه، الذي يعمل كأداة مركزية من أدوات السياسة الصناعية. فمن خلال الشركات التابعة، والمشاريع المشتركة، واتفاقيات الترخيص، والوسطاء المحليين، يتحرك هؤلاء الفاعلون عبر ولايات قضائية متعددة، مع تجزئة المساءلة. وهذه المرونة التنظيمية ليست عرضية؛ بل تعكس نمطاً من التنظيم الصناعي تُنشَر فيه أولويات الدولة عبر شركات تستطيع إعادة تشكيل بنيتها القانونية والمالية والعملياتية استجابةً للبيئات التنظيمية. وبهذا المعنى، تصبح الشركة بالمعنى الاقتصادي الآلية التي تُفعَّل من خلالها السياسة الصناعية ذات الطابع العسكري خارج الحدود الرسمية للدولة. فهي تتيح الوصول إلى الأسواق وتمكّن من الالتفاف على القيود التي كانت ستنطبق خلافاً لذلك على الفعل المباشر للدولة. وما يتبلور هنا ليس نموذج تصدير خطياً، بل بنية تحتية موزعة تُوجَّه من خلالها قدرات المراقبة، ويُعاد تجميعها، وتُدمج داخل أنظمة الحوكمة المدنية.

ثالثاً، تعمل مؤسسات التنمية متعددة الأطراف كواجهات حاسمة في هذه العملية. فمن خلال دمج مثل هذه الشركات في برامج مؤطرة بوصفها بناءً للقدرات الرقمية، أو مرونة سيبرانية، أو تحديثاً مؤسسياً، تسهّل هذه المؤسسات تطبيع تقنيات المراقبة كمكونات من مكونات الحوكمة المشروعة. وهي بذلك لا تموّل تبنّي التكنولوجيا فحسب؛ بل تشارك بصورة فاعلة في بناء أسواق جديدة للتقنيات ذات الطابع العسكري، من خلال إعادة صياغتها بوصفها محايدة وضرورية وتنموية.

من الاستعمار الاستيطاني والاحتلال بالتحكّم عن بُعد: الابتكار التكنولوجي، والصهيونية النيوليبرالية، والصمود الرقمي في زمن الإبادة الجماعية

أريس بشارة

أريس زميلة باحثة في قسم العلوم السياسية وعلم الاجتماع في المدرسة العليا العادية في بيزا. هي باحثة في علم الاجتماع السياسي والتنظيمي. يجسر عملها دراسات إسرائيل/فلسطين مع قضايا التكنولوجيا والنوع الاجتماعي والاستعمار الاستيطاني. شغلت مناصب بحثية في جامعة تل أبيب وجامعة ولاية ميشيغان والمعهد الجامعي الأوروبي، وغيرها.

يحمل مشروع أريس البحثي عنوان: «حجب فلسطين: كشف النفاق ونزع الإنسانية عبر بُنى القوة في زمن الإبادة»، ويحقق في كيفية مساهمة الحكومات والشركات والأوساط الأكاديمية في تكريس الرقابة ونزع الإنسانية عن فلسطين، خصوصًا عبر أدوات القوة التقنية والمؤسسية.

الملخّص

تستعرض هذه المقالة نظريًا الكيفية التي أعادت بها ديناميات التقاء الابتكار التكنولوجي والاستراتيجية العسكرية تشكيلَ الاحتلال الإسرائيلي في صورة استعمار استيطاني رقمي، وهو تحوّل أصبح أكثر وضوحاً بعد السابع من تشرين الأول 2023. ومن خلال النقاشات الموسعة حول الاستعمار الرقمي، تُبيّن الدراسة أنّ اقتصاد الابتكار الإسرائيلي يعمل، في آنٍ واحد، بوصفه مشروعًا وطنيًا ونموذجًا تجاريًا عالميًا، بما يُدرج قطاع التكنولوجيا في عنف الإبادة الجماعية. وانطلاقًا من دراسات الاستعمار الاستيطاني، ونظرية الاستعمار الرقمي، والبيوسياسة الفوكوية، وتحليل باومان للعنف المؤسسي، تصوغ المقالة مفهومَ الاحتلال بالتحكّم عن بُعد بوصفه نتاجًا للترابط بين المؤسسة العسكرية والأكاديمية وقطاع التكنولوجيا في ظلّ الصهيونية النيوليبرالية. وبالاستناد إلى تحليل المضمون الموضوعاتي، ومقابلات مع تقنيين فلسطينيين خلال الفترة 2020–2024، تحدّد المقالة ثلاثة أنماط للإبادة الرقمية: الجسدية (الاستهداف المدعوم بالذكاء الاصطناعي)، والاقتصادية (البحث والتطوير العسكري في الأسواق العالمية)، والمعرفية (الرقابة الرقمية). وفي المقابل، يطوّر الفلسطينيون صمودًا رقميًا، أي ممارسات مترابطة، قوامها التحمّل والمقاومة.

الكلمات المفتاحية: **الاستعمار الاستيطاني الرقمي؛ الصهيونية النيوليبرالية؛ الصمود الرقمي؛ الحالة المستقبليّة.**

١. المقدّمة

منذ مطلع الألفية، تناول عدد من الباحثين الاحتلال الإسرائيلي بوصفه نموذجًا إرشاديًا لحوكمة استعمارية استيطانية تقوم على منطق الإبادة (Lentin, 2020; Sabbagh-Khoury, 2022; Sa'di, 2021; Veracini, 2011, 2015; Wolfe, 2006). وفي فلسطين، فإنّ ما كان يعتمد تاريخيًا على الاستيلاء على الأرض، والحواجز العسكرية، والتنظيم الديمغرافي، بات يعمل بصورة متزايدة من خلال بنى تحتية للتحكّم عن بُعد، وتحليلات تنبؤية، وقواعد بيانات بيومترية، واستهداف مدعوم بالذكاء الاصطناعي. ففي غزة، والضفة الغربية، وفلسطين التاريخية، يتعاون العسكريون، والأكاديميون، والشركات على تطوير أنظمة جديدة من العنف الخوارزمي وإدارة السكان (Ahmad, 2021; Avis et al., 2025; Bevilacqua, 2022; Musleh, 2018; Sa'di, 2021; Shalhoub-Kevorkian, 2015, 2017; Shehadeh, 2023; Tawil-Souri, 2012; Zureik, 2016b, 2020; Zureik et al., 2010).

وقد اشتدّ هذا التحوّل بعد 7 أكتوبر 2023. فقد تزامن الهجوم الإبادي المستمر على غزة مع التوسّع في استخدام قوائم القتل الآلية، وأنظمة التعرّف إلى الوجوه، والحرب الجوية المدعومة بالآلات. وقد وصف ضباط إسرائيليون ذلك` بما اصبح يعرف «بالمطاردة الواسعة» مدعومة بالذكاء الاصطناعي، تُدمَّر فيها المنازل بناءً على وجود شخص مستهدف واحد فيها. ويجسّد ذلك تحليل باومان (Bauman, 1989) للعنف المؤسسي: أذى يُدار بيروقراطيًا على نحو يباعد بين مرتكبي الأذى ونتائج أفعالهم.

وقد تجاوزت هذه الأنظمة حدود إسرائيل بكثير. فالانتقال من "أمّة الشركات الناشئة (الستارت-أب)" المحتفى بها (Senor & Singer, 2009) إلى ما يمكن تسميته "أمّة التخارج" لم يكن ثمرة تحرير السوق وحده، بل أتاحته أيضًا عمليةٌ تنسيق مقصودة قادتها الدولة. ويبيّن ماغور (Maggor, 2020) أنّ اقتصاد الابتكار الإسرائيلي نشأ عبر نموذج تنموي جديد تتولّى فيه الدولة توجيه رأس المال وتنمية القدرات التكنولوجية العالية لإدماج الشركات في الأسواق العالمية. ويُفهَم هذا الاندماج بين العسكرة والابتكار هنا بوصفه صهيونية نيوليبرالية (Getzoff, 2020): تشكيلة تمزج عقيدة الأمن القومي بمنطق السوق والتفاؤل التكنولوجي، وتؤطّر «التكنولوجيا بوصفها صهيونية عملية»، وفقًا لتصريح غلعاد رابينوفيتش1.

ولا تُمثّل هذه التطورات مجرد ابتكارات عسكرية، بل هي أيضًا نتاج اقتصاد سياسي أوسع. فالنخب التكنولوجية الإسرائيلية لا تعمل على نحو متزايد بوصفها مستفيدة من سياسات الدولة فحسب، بل أيضًا بوصفها فاعلًا سياسيًا يسهم في تشكيلها. وكما يجادل شحادة (Shihadeh, 2024)، انتقل قطاع التكنولوجيا الفائقة من التأثير غير المباشر إلى بناء نفوذ مؤسسي مباشر، بما يعزّز السلطة التكنوسياسية داخليًا ويعمّق التشابكات العالمية في الوقت ذاته. ومن خلال نقل الأسلحة، وعقود الأمن السيبراني، وشراكات الذكاء الاصطناعي، وتدفّقات رأس المال الاستثماري المغامر، يربط الفاعلون التكنولوجيون الإسرائيليون الشركات متعددة الجنسيات والحكومات الأجنبية بمنظومة الأمن والابتكار الإسرائيلية (Loewenstein, 2023; Swed & Butler, 2015; Tariq, 2024; Tarvainen & Challand, 2024).

وتجعل هذه التشابكات الدولية الحكومات الأجنبية والشركات الخاصة متواطئةً بنيويًا في البنى التحتية للاحتلال. ويُظهر تقرير ألبانيزي (2025)،[2] من اقتصاد الاحتلال إلى اقتصاد الإبادة الجماعية، كيف تستفيد الأنظمةُ المؤسسية من التهجير والفصل العنصري والإبادة الجماعية وتُسهم في تمكينها، بما في ذلك عبر التقنيات مزدوجة الاستخدام مثل المراقبة البيومترية، وأدوات الاستهداف بالذكاء الاصطناعي، والمنصات العسكرية السحابية التي تحوّل الأرض المحتلة إلى حقل تجارب.

واستنادًا إلى ألبانيزي (2025)[3] وإلى هيلغا طويل- الصوري (Tawil-Souri, 2012)، التي نظّرت لغزة بوصفها «حيّزًا احتوائيًا عالي التقنية»، تضع هذه المقالة الهيمنةَ الإسرائيلية المعاصرة ضمن تأطير أوسع للاستعمار الاستيطاني الرقمي. فغزة تمثّل مثالًا لحيّزٍ يلتقي فيه الحصار المادي مع التحكّم الرقمي والبيومتري والبنيوي، بحيث تصبح المنطقة في آنٍ واحد معزولةً، وخاضعةً للمراقبة، ومعتمدةً تكنولوجيًا. وبالاستناد إلى دراسات الاستعمار الاستيطاني (Lentin, 2020; Sabbagh-Khoury, 2022; Sa'di, 2021; Veracini, 2011, 2015; Wolfe, 2006)، وأدبيات الاستعمار الرقمي (Bevilacqua, 2022; Couldry & Mejias, 2019; Kwet, 2019, 2022)، وبالاستئناس بالبيوسياسة الفوكوية (Foucault, 2008) ونظرة باومان إلى العنف المؤسسي (Bauman, 1989)، تطرح هذه المقالة حجتين أساسيتين.

1 غلعاد رابينوفيتش هو مُستثمر إسرائيلي في قطاع التقانة العُليا (هاي-تك).

2 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

3 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

أولًا، دخل الاحتلال مرحلةً تتوسّطها المنظومات الرقمية، يمتدّ فيها منطق الاستعمار الاستيطاني إلى الحوكمة الخوارزمية. ففي ظلّ الصهيونية النيوليبرالية، تُضفي التكنولوجيا شرعية على العنف وتوسّع نطاقه، بينما تُدرِج الاحتلال في أسواق الذكاء الاصطناعي والأمن العالمية. كما أنّ التشابك المدني–العسكري–الأكاديمي يُنتج، على نحوٍ مشترك، أنظمةَ مراقبة تجعل الحياة الفلسطينية مكشوفة بصورة مفرطة للآلة، في الوقت الذي تزيل فيه قدرتهم على الفعل السياسي.

ثانيًا، يمارس الفلسطينيون الصمود الرقمي، وهو جملة من الممارسات التكنولوجية الصامدة التي ترفض المحو وتؤكد الحضور الجمعي. فالناشطون، والتقنيون، والتجمعات الأهلية يطوّرون بنى تحتية مضادّة — من منصات الأرشفة، إلى الشبكات المتداخلة، إلى الحملات الرقمية العابرة للحدود — بما يصون قدرتهم على الفعل السياسي في ظلّ الرقابة، والانقطاع، والعنف. وفي الوقت الذي توظّف فيه المؤسسات الإسرائيلية الأنظمةَ الخوارزمية لتفتيت الحضور الفلسطيني وإسكاته، يعيد الفلسطينيون توظيف الأدوات الرقمية من أجل الصمود، والتوثيق، والإتصال.

وعليه، تتناول هذه الدراسة سؤالين رئيسيين:
1. كيف يُفعِّل اقتصاد الابتكار الإسرائيلي، في تشابكه مع المؤسستين العسكرية والأكاديمية، الاستعمارَ الاستيطاني الرقمي في ظلّ الإبادة الجماعية المستمرة؟
2. كيف يُفعّل الفلسطينيون الصمود الرقمي لمقاومة التقنيات المصممة لإزالتهم جسديًا، وتجريدهم من إنسانيتهم، وإسكاتهم، وتقويضها وإعادة تأويلها؟

ومن خلال معالجة هذين السؤالين، تُسهم المقالة في الأدبيات المتعلقة بالتكنولوجيا والابتكار، والاستعمار الاستيطاني، والصمود الفلسطيني، وذلك عبر موضعة البنى التحتية الرقمية ضمن الهرميات العالمية للسلطة والمقاومة.

٢. مراجعة الأدبيات

2.1 الاستعمار الاستيطاني في العصر الرقمي: الحوكمة الخوارزمية، والبيوسياسة، والإبادة المادية

تفترض نظرية الاستعمار الاستيطاني أنّ «منطق الإبادة» هو البنية الأساسية الهادفة إلى التخلص من السكان الأصليين وإحلال نظام سياسي جديد محلّهم (Wolfe, 2006; Veracini, 2011, 2015; Sabbagh-Khoury, 2022). وفي فلسطين، تجلّى هذا المنطق منذ زمن طويل في مصادرة الأراضي والمراقبة القائمة على أسس عنصرية (Ahmad, 2021; Shalhoub-Kevorkian, 2015; Zureik, 2001, 2016b, 2016a; Zureik et al., 2010).

وخلال العقدين الأخيرين، خضعت هذه البنية لتحوّل رقمي، بحيث لم تعد آليات السيطرة المادية، مثل الحواجز والدوريات، تعمل وحدها، بل باتت تُستكمَل أو تُستبدَل بأنماط من الحوكمة الخوارزمية، تشمل قواعد البيانات البيومترية، والتحليلات التنبؤية، وأنظمة الاستهداف المؤتمتة (Loewenstein, 2023; Musleh, 2018; Zureik, 2001, 2016b; Zureik et al., 2010).

ويجب النظر إلى هذا التحوّل من منظور بيوسياسي (Foucault, 2008)، حيث يُفهَم الاستعمار الاستيطاني الرقمي بوصفه اندماجًا بين الهيمنة الاستيطانية والبنى التحتية التكنولوجية. فالْحَوكمة الخوارزمية توسع منظور السيادة الاستيطانية إلى صيغ حاسوبية تُدير وتُصنّف وتستهدف الفلسطينيين، بما يترجم الإبادة إلى شيفرة حاسوب. ومن المهم الإشارة إلى أنّ هذه العملية تُسهل «العنف المؤسسي» (Bauman, 1989)، إذ إنّ نزع القدرة البشرية عبر الأنظمة المؤتمتة يخلق مسافةً أخلاقية، فيُختزل الضحايا إلى مجرد بيانات، ويغدو تنفيذ العنف عمليةً ميكانيكية. وفي موازاة ذلك، تؤكد أدبيات الاستعمار الرقمي أنّ هذه البنى التحتية لا تستبدل دوائر الهيمنة التقليدية، بل تُكثّفها (Gillespie, 2018, 2018; Kwet, 2019, 2022; Noble, 2018, 2018; Tarvainen & Challand, 2024)، بما يعيد إنتاج تواريخ راسخة من العنصرية والإخضاع الاقتصادي في ظل الأيديولوجيات النيوليبرالية (Clarno, 2018b, 2018a; Johnson, 2019; Lloyd & Wolfe, 2016; Wildeman, 2019).

2.2 الصهيونية النيوليبرالية والاقتصاد السياسي للابتكار التكنولوجي

إنّ استدامة الاستعمار الاستيطاني الرقمي تقوم على اقتصاد سياسي متكامل. فقد جرى بناء قطاع التكنولوجيا المتقدمة الإسرائيلي، الذي كثيرًا ما يُروَّج له ضمن سردية «أمة الشركات الناشئة» (Senor & Singer, 2009)، من خلال استثمارات دولة منسقة، وبحث وتطوير عسكري، ورأس مال مغامر (Maggor, 2020). وقد أفضى ذلك إلى نشوء مُركّب مدني–عسكري–أكاديمي قوي، تؤدي فيه الوحدات العسكرية، مثل الوحدة 8200، دور الحاضنات التي تحوّل أدوات المراقبة العسكرية إلى منتجات تجارية، غالبًا ما تُجرَّب على الفلسطينيين ثم تُسوَّق بوصفها "مجرَّبة ميدانيًا" (Loewenstein, 2023; Swed & Butler, 2015; Wind, 2024).

وتُعرَّف هذه البنية بوصفها الصهيونية النيوليبرالية (Getzoff, 2020)، وهي صيغة تمزج بين العقيدة الأمنية ومنطق السوق، وتعيد تأطير الابتكار التكنولوجي بوصفه خدمةً وطنية، أي «التكنولوجيا بوصفها صهيونية عملية». ويُنتج هذا المحرّك الاقتصادي تبعيةً بنيوية للفلسطينيين، الذين يُوضَعون في موقع الخاضعين للمراقبة والعمالة المتعاقدة من الباطن تحت خطاب «بناء السلام الاقتصادي» (Last, 2007). كما يتجه هذا الاقتصاد السياسي إلى مزيد من العولمة عبر الشراكات متعددة الجنسيات، بما يُدمج الشركات العالمية في البنى التحتية للاحتلال. والمركّب نفسه الذي يحكم التبعية الاقتصادية هو الذي يحكم أيضًا إنتاج المعرفة، بما يخلق الشروط اللازمة للنمطين الثاني والثالث من الإبادة.

2.3 الإبستمولوجيا، والأرشيفات، وإعادة إنتاج المعرفة

إنّ الأنظمة الاقتصادية والبيوسياسية المشار إليها أعلاه تُصان بواسطة بنية تحتية إبستيمية تُضفي الشرعية على الهيمنة. ويُقاوَم العنف الإبستمولوجي (Fanon, 1963) من خلال الفعل الإبستيمي/المعرفي المقاوم (Mignolo, 2009, 2011; Mignolo & Walsh, 2018). وفي السياق الإسرائيلي، تؤدي المؤسسات الأكاديمية والإعلامية دور أنظمة معرفة مُعسكَرة (Wind, 2024)، إذ تفرض تراتبية إبستيمية تُعلي من السرديات الصهيونية وتهمّش التاريخ الفلسطيني أو تُجرّمه (Peled-

(Elhanan, 2012; Sabbah-Karkabi & Abu-Rabia-Queder, 2025). ويتضخّم هذا النمط من الإبادة بفعل السرديات الاحتفائية العالمية (Senor & Singer, 2009) التي تُقدّس التقدّم التكنولوجي الإسرائيلي وتغض النظر عن أوضاعه الاستعمارية.[4]

وفضلًا عن ذلك، تتجلّى الهيمنة الإبستيمية في السيطرة على الأرشيف. فبينما دأبت إسرائيل تاريخيًا، منذ النكبة، على مصادرة المقتنيات الثقافية الفلسطينية المادية وتدميرها (Amit, 2011; Masalha, 2012; Sela, 2018)، فقد صعّد العدوان الإبادي الراهن ذلك إلى مستوى الإبادة المنهجية للبيانات الرقمية. إنّ استهداف الجامعات والخوادم في غزة، والذي وُصف بأنه إبادة تعليمية (Giroux, 2025) (scholasticide)، يمثّل الحافة الأكثر تطرفًا للاستعمار الاستيطاني الرقمي. فالمسألة لا تتعلق فقط بتدمير المباني، بل بمحاولة محو «التوأم الرقمي» للمجتمع الفلسطيني عبر حذف الأرشيفات السحابية، والسجلات الأكاديمية، والذاكرة الرقمية. ومع اقتران ذلك بالحوكمة الخوارزمية ورقابة المنصات، ينشأ نمط من الإزالة الرقمية الإبستيمية: عملية تُدار عن بُعد تجعل الحياة الفلسطينية غير قابلة للعثور عليها رقميًا وغير مرئية، بما يضمن أن يتبع تدمير الجسد المادي محوٌ مؤتمت لتاريخه ومستقبله من السجل الرقمي العالمي.

2.4 القمع الرقمي، والصمود، وإنهاء الاستعمار

يُكمّل القمع الرقمي أنماطَ السيطرة التقليدية التي تمارسها الدولة، من خلال تقييد الخطاب على الإنترنت، ومراقبة الاتصالات، والرصد، إلى جانب الإعتقال والرقابة (Awwad & Toyama, 2024). وفي هذا السياق، يمدّ النظام التكنو-استعماري الإسرائيلي أنظمة الهيمنة الراسخة إلى الفضاء الرقمي. ومع ذلك، تكشف الممارسات الرقمية الفلسطينية كيف تعمل المساحات الإلكترونية بوصفها ساحات للنشاط السياسي، والمقاومة، والتنقّل المهني (Althalathini & Tlaiss, 2023; Aouragh, 2011; Tawil-Souri & Aouragh, 2014; York, 2012). فالنشاط الرقمي يخلق إمكانات تشاركية عبر تمكين المشاركة المستقلة والعابرة للحدود والمشاركة الجماعية (Awwad & Toyama, 2024)، كما يمكن للانخراط التكنولوجي أن يؤدي وظيفةً من وظائف الفاعلية والقدرة على التأثير (Rindova et al., 2009).

غير أنّ هذه الإمكانات تواجه قيود، على سبيل المثال عدم المساواة في الوصول، وغرف الصدى، والهشاشة أمام المراقبة. ويؤدي القمع الرقمي إلى تعميق هذه القيود من خلال حوكمة المنصات، والتحكم الخوارزمي، ومحو البنى التحتية الثقافية (Awwad & Toyama, 2024). وتشكل هذه الديناميات ما يمكن تسميته الإزالة الرقمية الإبستيمية، أي الانتقاص المنهجي من قيمة المعرفة الفلسطينية.

كما تُبرز الدراسات أنّ ضبط المحتوى، والترتيب الخوارزمي، والتصنيف المؤتمت، تعمل بوصفها بنى تحتية إبستيمية تحدد ما الذي يكون مرئيًا، وموثوقًا، وقابلًا للتداول والمشاركة (Peeters & Schuilenburg, 2023). وفي الحالة الفلسطينية، تُظهر أبحاث المجتمع المدني نمطًا من اللاتماثل الإبستيمي الخوارزمي: إذ يُقيَّد

4 See Books such as Let There Be Water (Siegel M., 2015), and Thou Shalt Innovate (Jorisch, 2018) frame Israeli technological development as a civilizational mission to "make the desert bloom" or "repair the world," sacralizing innovation as moral virtue while erasing the colonial conditions that enable it. These narratives present technological progress as evidence of national genius and divine favor, thereby legitimizing Israel's global techno-political authority and obscuring Palestinian dispossession. In this configuration, tech discourse itself functions as a **mode of epistemic reproduction**, stabilizing Zionist myths and marginalizing Palestinians as either absent, irrelevant, or "politicized".

المحتوى الفلسطيني بصورة غير متناسبة، في حين يستمرّ التحريض ضد الفلسطينيين، إلى حد كبير، من دون مساءلة تُذكر (7amleh, 2024; Ahmad, 2021; Al-Salhi, 2021).

وتُميّز الأبحاث الخاصة بفلسطين بين نشاطٍ يهدف إلى توسيع الوصول الرقمي، وآخر يستخدم المنصات الرقمية لتحقيق أهداف سياسية. أما النمط الثاني، والذي غالبًا ما يُوصَف بأنه «انتفاضة إلكترونية» (Aouragh, 2011; Tawil-Souri & Aouragh, 2014)، فيشمل تداول الشهادات، وتوثيق العنف، والدفع بحملات عالمية مثل حركة المقاطعة وسحب الاستثمارات وفرض العقوبات. وقد أصبحت وسوم مثل #GazaUnderAttack أدوات أساسية للشهادة الحية والمناصرة العابرة للحدود.

وتتداخل هذه الممارسات مع مفهوم الصمود، الذي دلّ تاريخيًا على الرفض الثابت للتخلي عن الأرض أو الهوية (Abu-Lughod, 2020; Busse, 2022; Hammami, 2005; Rijke & Van Teeffelen, 2014; Tatour, 2019). أما رقميًا، فيعني الصمود مقاومة المحو ومواجهة القمع الخوارزمي (Khoury-Machool, 2007; Shehadeh, 2023). وتقوم مشاريع مثل Visualizing Palestine وPalestine Open Maps و Encyclopedia of the Palestine Question بإعادة بناء تواريخ جرى قمعها، بينما تعمل مؤسسات مثل حملة على تحدي الرقابة؛ وهي جميعًا أشكال من السيادة الإبستيمية.

كما يعمل الصمود الرقمي بوصفه شكلًا من العصيان الإبستيمي المنسجم مع مبادئ التصميم المناهض للاستعمار (Mignolo, 2009, 2011; Mignolo & Walsh, 2018)، ويتناغم مع النقد العالمي للاستعمار البياني (Couldry & Mejias, 2019; Milan & Treré, 2019). وتعكس مفاهيم مثل "الوطن الرقمي العائم" عند شحادة (Shehadeh, 2023)، «والمقاومة الإلكترونية» عند خوري-مخول (Khoury-Machool, 2007)، الكيفية التي يخلق بها الفلسطينيون فضاءات رقمية مشتركة عبر جغرافيات ممزقة. وبعد 7 أكتوبر 2023، ازدادت هذه الممارسات كثافةً مع تداول الشهادات رغم انقطاعات الاتصال والقمع الخوارزمي، فتحوّلت أنظمة المراقبة ذاتها إلى بنى تحتية للشهادة والحشد والتعبئة (Aouragh, 2011; Khoury-Machool, 2007).

٣. المنهجية

تعتمد هذه الدراسة تصميمًا نوعيًا قائمًا على مناهج مختلطة، بهدف معالجة السؤالين البحثيين المتعلقين بالاستعمار الاستيطاني الرقمي والصمود الرقمي. وانطلاقًا من مناهج بحثية تفكيكية/مناهضة للاستعمار، يتعامل التحليل مع أنظمة الذكاء الاصطناعي وأطر حوكمة البيانات بوصفها تشكيلات اجتماعية-تقنية يصوغها منطق العسكرة والإبادة.

3.1 تصميم البحث والبيانات

تدمج هذه الدراسة بين مقاربتين متكاملتين:

1. التحليل الموضوعاتي للخطاب والمحتوى للتقارير الاستقصائية والتغطيات

الإعلامية خلال الفترة (2020–2025)، عبر خمس فئات هي: (الاستهداف بالذكاء الاصطناعي، والرقابة، والتواطؤ الأكاديمي، والصمود الرقمي). (راجع التقرير كاملًا بهذا الرابط) كما جرى تحليل أرشيف مُنتقى من منشورات متاحة للعامة على وسائل التواصل الاجتماعي نشرها سكان من غزة خلال الفترة (تشرين الأول 2023 – شباط 2024)، وذلك لفهم الخبرات المعاشة للحرب الرقمية. 2. مقابلات شبه منظّمة مع خمسة عشر تقنيًا/ة فلسطينيًا/ة (تم اختيارهم من مجموعة بيانات تضم سبعين مقابلة أُجريت بين 2020 و2024) من غزة، والضفة الغربية/القدس الشرقية، وأراضي 1948. وقد استُخدمت تقنية العيّنة المتسلسلة (Snowball Sampling)، وأُجريت المقابلات باللغة العربية، مع الالتزام الصارم بحماية هوية المشاركين وضمان سريتهم.

ويتيح هذا التصميم تقديم قراءة متعددة المستويات لكيفية إسهام البنى التحتية الرقمية في ترسيخ السلطة الاستعمارية الاستيطانية، بالتوازي مع توثيق أشكال الصمود الرقمي.

3.2 الإجراءات التحليلية

جُمعت البيانات، ورُمّزت، ثم نُظّمت في فئات موضوعاتية باستخدام برنامج ATLAS.ti. وركّز التحليل على تقاطع المؤسسات العسكرية، وشركات التكنولوجيا الخاصة، والمؤسسات الأكاديمية، وعلى الآليات الخطابية التي تنزع الطابع السياسي عن التكنولوجيا، في الوقت الذي تُنتج فيه الإقصاء والتجريد من الإنسانية. وقد جمع الترميز بين استراتيجيات استنباطية (مستندة إلى المفاهيم النظرية في الأدبيات العلمية) ومقاربات استقرائية. كما خضعت المقابلات للتحليل باستخدام استراتيجيات سردية، من أجل تحديد اللحظات التي يتكيّف فيها التقنيون مع القيود، أو يقاومونها، أو يعيدون تشكيلها داخل المشهد التكنولوجي الاستعماري الاستيطاني.

٤. النتاج والمناقشة

تُظهر نتائج هذه الدراسة أنّ الاحتلال الإسرائيلي قد تطوّر ليصبح نموذجًا إرشاديًا للاستعمار الاستيطاني الرقمي. ففي هذا التشكّل، لا تحلّ الأنظمة الخوارزمية، والبنى التحتية الرقمية، واقتصادات الابتكار، محلّ الوظائف العسكرية أو البيروقراطية التقليدية، بل تعمل بوصفها طبقةً استعمارية مُضافة من السلطة تُسرّع عمليات المراقبة والتحكّم والإبادة وتوسّع نطاقها. وبناءً على ذلك، بات الاحتلال يعمل على نحو متزايد من خلال الاستهداف المدفوع بالذكاء الاصطناعي، والمراقبة البيومترية، والتحكّم الشبكي، بما يُجسّد تلاقي الحداثة التكنولوجية مع الهيمنة الاستعمارية. وتوسيعًا لحجة وولف (Wolfe, 2006)، تُبيّن هذه الدراسة أنّ "منطق الإبادة" يتكشف في الوقت نفسه عبر الحدود المكانية والرقمية. ففي ظل هذا النظام، يصبح الفلسطينيون مرئيين على نحو مفرط بوصفهم موضوعات بيانات، لكنهم غير مرئيين سياسيًا؛ وهي مفارقة تعكس أبارتهايدًا مؤتمتًا تُترجم فيه السيطرة المُعنصَرة إلى صيغ حاسوبية. كما أنّ الأنظمة الخوارزمية التي تنظّم الحركة، والوصول، والظهور، تُدرج منطق الإزالة مباشرةً في البنى التحتية الرقمية. وهذا يكشف حدود الخطاب حول الذكاء الاصطناعي «الأخلاقي» إذ يعمل الذكاء

الاصطناعي هنا بوصفه امتدادًا فتاكًا للسلطة الاستيطانية، حيث تُخفي «الدقة» عنف الدولة. ويحلّل القسم التالي ثلاثة أنماط للإزالة الرقمية (الجسدية، والاقتصادية، والإبستيمية/المعرفية) ويستكشف كيف يُفعّل الفلسطينيون الصمود الرقمي لمقاومة تقنيات التحكّم هذه وتقويضها.

4.1 ثلاثة أنماط للإبادة

4.1.1 الإبادة المادية: الاستهداف الخوارزمي، والحرب المدعومة بالذكاء الاصطناعي، والمراقبة، والاحتلال بالتحكّم عن بُعد

يوسّع هذا القسم أطر الاستعمار الاستيطاني والاستعمار الرقمي من خلال إظهار الكيفية التي تترجم بها المراقبة البيومترية والاستهداف بالذكاء الاصطناعي منطقَ الإبادة إلى أنظمة حاسوبية. فأنظمة مثل Blue Wolf وRed Wolf وWolf Pack تُنشئ نظامَ مراقبةٍ متكاملًا عبر الأرض الفلسطينية المحتلة، وهو ما تصفه منظمة العفو الدولية بأنه «أبارتهايد مؤتمت»، يكرّس الفصل العنصري على نحو مؤسسي.[5]

يُتيح برنامج Blue Wolf678 للجنود تصوير الفلسطينيين وإجراء مطابقة فورية مع قواعد البيانات البيومترية. كما يتضمن التطبيق «لوحة المتصدرين» تكافئ الوحدات العسكرية بحوافز، مثل إجازات مدفوعة، عند التقاط أكبر عدد من الوجوه.[9][10] وقد حذّرت منظمة العفو الدولية من أنّ الفلسطينيين يواجهون «خطر أن تتعقبهم خوارزمية أو تمنعهم من دخول أحيائهم».[11] أمّا نظام Red Wolf، المُركّب عند حواجز الخليل، فيقرر السماح بالعبور ويُدرج الفلسطينيين تلقائيًا في قواعد البيانات من دون موافقتهم. وقد أشار أحد السكان إلى أنّ الجنود يستطيعون منع شخص من دخول منزله نفسه بذريعة أنه «غير موجود في قاعدة البيانات».[12]

وتجسّد هذه التقنيات ما يسميه فوكو (Foucault, 2008) بالبنى التحتية الإبستيمية/المعرفية، حيث تُدمج السلطة الاستعمارية في الشيفرة البرمجية. ويخلص تقرير صادر عن حملة إلى أنّ هذا النمط يُعمّق انعدام الأمان والعسكرة

5 منظمة العفو الدولية. 2023. الفصل العنصري المؤتمت: استخدام إسرائيل لتقنيات التعرّف على الوجه في الأراضي الفلسطينية المُحتلة. https://www.amnesty.org/en/documents/mde15/6701/2023/en/

6 ميدل إيست آي. 18 آذار/ مارس 2021. إسرائيل: ما هو تطبيق بلو وولف؟ يستخدمه الجنود لتصوير الفلسطينيين. Middle East Eye. https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians

7 هآرتس. 2 أيار/ مايو 2023. منظمة العفو الدولية تقول إن اسرائيل تستخدم تقنية التعرف على الوجوه لتعميق الفصل العنصري. هآرتس. https://www.haaretz.com/israel-news/2023-05-02/ty-article/highlight/israel-using-facial-recognition-tech-to-entrench-apartheid-amnesty-intl-says/00000187-db8a-d9b4-abaf-fbbe6c080000

8 ذي جارديان، 19 نيسان/ أبريل 2019. كيف توّظف اسرائيل أنظمة التعرّف على الوجه في غزة وأبعد منها. ذي جارديان. https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians

9 ذي جارديان، 19 نيسان/ أبريل 2019. كيف توّظف اسرائيل أنظمة التعرّف على الوجه في غزة وأبعد منها. ذي جارديان. https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians

10 ميدل إيست آي. 9 تشرين الثاني/ نوفمبر 2021. تعرّف على بلو وولف، التطبيق الاسرائيلي المُستخدم للتجسس على الفلسطينيين في الأراضي الفلسطينية المُحتلة بالضفة الغربية. Middle East Eye. https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians

11 منظمة العفو الدولية. 2 أيار/ مايو 2023. إسرائيل/ الأراضي الفلسطينية المُحتلة: السلطات الاسرائيلية تستخدم تقنيات التعرّف على الوجوه لتعميق الفصل العنصري. Amnesty International. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

12 منظمة العفو الدولية. 2 أيار/ مايو 2023. إسرائيل/ الأراضي الفلسطينية المُحتلة: السلطات الاسرائيلية تستخدم تقنيات التعرّف على الوجوه لتعميق الفصل العنصري. Amnesty International. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

تحت غطاء الأمن.[13] وكما ترى طويل- الصوري (Tawil-Souri, 2012)، تعمل الفضاءات الفلسطينية بوصفها «حيز احتوائي عالية التقنية»، بما يعكس النظامَ البيروقراطي والتكنولوجي الذي يتوسّط العنفَ الاستعماري.

وإضافة إلى ذلك، توسّع أنظمة الاستهداف المدعومة بالذكاء الاصطناعي هذا المنطق من خلال تحويل فلسطين إلى مختبر لحرب الكترونية. وكما أوضح أفنير بن زاكين، رئيس شعبة التكنولوجيا واللوجستيات في الجيش الإسرائيلي: «إذا كنت أطور منتجًا وأريد اختباره ميدانيًا، فكل ما عليّ فعله هو أن أذهب خمسة أو عشرة كيلومترات... وتُعتبر غزة موقعًا لاختبار معدات القتال الكنولوجية (Musleh, 2018). ويتوافق ذلك مع أبحاث تُظهر أنّ اقتصاد الابتكار الإسرائيلي متشابك مع الاختبار الميداني العسكري وتصدير التقنيات مزدوجة الاستخدام (Kwet, 2022; Tarvainen & Challand, 2024).

وتوثّق عدة تقارير[14][15][16] أنظمةً مثل Lavender و?Where's Daddy وThe Gospel. وقد طوّرتها الوحدة 8200، حيث حدّدت عشرات آلاف الفلسطينيين بوصفهم أهدافًا، مع حدٍّ أدنى من الرقابة البشرية. ووصف أحد الضباط إدخال مئات الأسماء إلى النظام، وسمّاهم «أهدافًا قمامية»، ثم قصف الأفراد حال تحديد وجودهم في منازلهم.[17]

كما تصف تقارير موازية نموذجًا لغويًا كبيرًا شبيهًا بـ»شات جي بي تي» يقوم بأتمتة تحليل التهديدات وتوليد قوائم الاعتقال.[18] وكما صرّح نديم ناشف: «لقد أصبح الفلسطينيون موضوعاتٍ في مختبر إسرائيل».[19] وتطمس هذه الأنظمة الحدود بين المدنيين والمقاتلين، وتتيح «مطاردة واسعة النطاق». وهي بذلك تجسّد مفهوم باومان (Bauman, 1989) للعنف المؤسسي، حيث يصبح القتل إجراءً روتينيًا ومنزوع من أي صفة أخلاقية مباشرة.

4.1.2 الإبادة الاقتصادية: قطاع التكنولوجيا، والأكاديميا، والعسكري

يحلّل هذا القسم «اقتصاد الاحتلال» - وتصعيده الأخير إلى ما تسميه ألبانيزي[20](Albanese, 2025) "اقتصاد الإبادة الجماعية" - من خلال عدسة الصهيونية النيوليبرالية. فهذا المشروع الأيديولوجي يدمج قطاع التكنولوجيا الفائقة، والجهاز

13 حملة. 19 كانون الأول/ ديسمبر 2023. صناعة التجسس الاسرائيلية وحقوق الانسان: الآثار على الفلسطينيين والعالم. مركز حملة. https://7amleh.org/post/7amleh-center-issues-a-report-on-israel-s-surveillance-industry-and-its-impact-on-human-rights

14 مجلة 972+. 13 نيسان/ أبريل 2024. Lavender AI: كيف يوّظف الجيش الإسرائيلي أنظمة الذكاء الاصطناعي في غزة. 972+ Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

15 ذي جارديان. 3 نيسان/ أبريل 2024. «الآلة فعلتها ببرودة: إسرائيل استخدمت الذكاء الاصطناعي للتعرّف على 37,000 شخصية مُستهدفة من حماس. The Guardian. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

16 ألبانيزي. ف. 2025. من اقتصاد الاحتلال إلى اقتصاد الإبادة: تقرير المقررة الخاصة لوضع حقوق الانسان في الأراضي الفلسطينية المُحتلة منذ العام 1967. الأمم المُتحدة. https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/

17 مجلة 972+. 13 نيسان/ أبريل 2024. Lavender AI: كيف يوّظف الجيش الإسرائيلي أنظمة الذكاء الاصطناعي في غزة. 972+ Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

18 مجلة 972+. 6 آذار/ مارس 2025. إسرائيل تطوّر أداة شبيهة بـ ChatGPT تسّلح التجسس على الفلسطينيين. 972+ Magazine. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/

19 مجلة 972+. 6 آذار/ مارس 2025. إسرائيل تطوّر أداة شبيهة بـ ChatGPT تسّلح التجسس على الفلسطينيين. 972+ Magazine. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/

20 ألبانيزي. ف. 2025. من اقتصاد الاحتلال إلى اقتصاد الإبادة: تقرير المقررة الخاصة لوضع حقوق الانسان في الأراضي الفلسطينية المُحتلة منذ العام 1967. الأمم المُتحدة. https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/

العسكري، والمؤسسات الأكاديمية، من أجل ترسيخ نظام استعماري استيطاني يقوم على تكريس السيطرة على الأرض واستغلال العمل الرقمي.

المسار المدني–العسكري–الأكاديمي

في ظل هذا النظام، لا تقف الجامعات الإسرائيلية وشركات التكنولوجيا الخاصة على هامش الدولة فحسب، بل تشكّل مراكز مندمجة بنيويًا تُطوَّر فيها أنظمة الأسلحة والمراقبة، وتُختبر ميدانيًا على الفلسطينيين، ثم تُسوَّق لاحقًا في السوق العالمية. وتذهب ألبانيز (Albanese, 2025) إلى أنّ هذه المؤسسات «هيّأت الشروط اللازمة لإبادة الفلسطينيين» من خلال توفير الأسس التقنية لعنف الدولة.

وتستضيف الجامعات الإسرائيلية شراكات بحث وتطوير مع شركات الأسلحة مثل Elbit Systems وRafael وتعمل بوصفها قنوات تجنيد لوحدات الاستخبارات العسكرية. وتشير مروة إلى أنّ المهندسين الفلسطينيين يشعرون في معارض التوظيف الجامعية، التي تهيمن عليها الشركات المتعاقدة مع الجيش، بأنهم «غرباء، ولا ينتمون»، وهو شعور يردده أيضًا ناشطون يصفون الجامعة بأنها «شريك في تعزيز آليات الاحتلال الإسرائيلي».[21]

ولا يقتصر دور هذه المؤسسات على التوظيف، بل تضطلع بدور عملياتي مباشر في الحرب. فقد أظهرت تقارير متعددة[22][23][24] الدور المباشر للجامعات في تطوير الأسلحة، وصياغة عقائد مثل «عقيدة الضاحية»، ومبادرات زمن الحرب مثل «غرفة الحرب الهندسية» (شاهد الفيديو) في جامعة تل أبيب، إلى جانب حملات الدعاية والدعم المادي للجنود في جامعة حيفا.[25] وكما تبيّن مايا ويند (Wind, 2024)، فإن هذه المؤسسات تقمع أيضًا الحقوق الأكاديمية الفلسطينية، في الوقت الذي تعزّز فيه بنى الأبارتهايد. وقد صرّح طلاب فلسطينيون في الأكاديميا الإسرائيلية لـ Middle East Eye[26] بأنهم يشعرون بعزلة متزايدة في الحرم الجامعي.

وقال أحدهم، الذي فضّل عدم الكشف عن هويته خشية تعليق دراسته بسبب تصريحاته:

"أمشي في الجامعة وأنا أعلم أن بعض زملائي يشاركون في غرف الحرب، ويصممون وسائل أكثر كفاءة لتنفيذ الإبادة الجماعية في غزة. إن هذا الزواج بين العسكرة والمؤسسات التعليمية يجعل من الصعب جدًا أن أنخرط بجدية في دراستي، لأنني أجد نفسي باستمرار أتساءل عن الأيديولوجيا الكامنة وراء ما نتعلمه".

21 كوجان. ي. 7 نيسان/ أبريل 2022. أكاديميا، أسلحة واحتلال: كيف تخدم جامعة تل أبيب مصالح الجيش والصناعات العسكرية. (باللغة العبرية). «زو هديرخ». https://zoha.org.il/111858/

22 حركة المقاطعة. المقاطعة الأكاديمية. BDS Movement. https://bdsmovement.net/academic-boycott

23 New Profile. (2025). Academia under orders: Militarism in Israeli academia — The collaboration between Israeli academia, the security establishment, and the military industry. [In Hebrew]. https://drive.google.com/file/d/14ZfAZn-ldt3hQSbtqegNoxE3uLHZoXlS/view

24 كيشنر، أ. 5 كانون الأول/ ديسمبر 2024. جامعة تل أبيب طوّرت كاميرات للكلاب لاستخدام وحدة عسكرية مرتبطة بالهجمات على غزة. ميدل ايست آي. https://www.middleeasteye.net/news/tel-aviv-university-developed-dog-cameras-army-unit-linked-gaza-attacks

25 الجزيرة. 10 أيلول/ سبتمبر 2024. التعليم الأكاديمي الاسرائيلي متورط مباشرة بجرائم الدولة. الجزيرة. https://www.aljazeera.com/opinions/2024/9/10/israeli-academia-is-directly-complicit-in-the-crimes-of-the-state

26 كيشنر، أ. 5 كانون الأول/ ديسمبر 2024. جامعة تل أبيب طوّرت كاميرات للكلاب لاستخدام وحدة عسكرية مرتبطة بالهجمات على غزة. ميدل ايست آي. https://www.middleeasteye.net/news/tel-aviv-university-developed-dog-cameras-army-unit-linked-gaza-attacks

ويُسنَد هذا النظام المعرفي المُعسكَر بدعم دولي كبير، بما في ذلك التمويل الأوروبي. إذ توفّر المؤسسات الأوروبية (مثل Horizon Europe بما يزيد على 2.12 مليار يورو) [27] والمؤسسات الأمريكية تمويلًا واسعًا، بما يزيد من إدماج هذه المؤسسات داخل الجهاز العسكري.[28] ويؤدي قطاع التكنولوجيا الفائقة، المتجذر في الاستخبارات العسكرية، دورًا محوريًا في القمع المؤتمت (مثل NSO Group وIBM). ووفقًا لعدة تقارير،[29][30][31][32] كثّف Project Nimbus (غوغل وأمازون) وMicrosoft Azure دعمهما للعمليات القتالية. وقد أدّت احتجاجات الموظفين تحت شعار No Tech for Apartheid ضد تواطؤ الشركات إلى موجات فصل جماعي،[33][34][35][36][37] الأمر الذي يبرز التشابك البنيوي للبنية التحتية للشركات مع الاحتلال، ويُسهل الانتقال من «اقتصاد الاحتلال» إلى «اقتصاد الإبادة الجماعية».[38]

وفي المحصلة، تؤدي الأكاديميا الإسرائيلية وظيفةَ مركز بحث وتطوير رئيسي للبنية التحتية الرقابية التابعة للدولة. فجامعات مثل التخنيون وجامعة تل أبيب تحتضن مختبرات متخصصة تُطوَّر فيها أنظمة بيومترية مدفوعة بالذكاء الاصطناعي وخوارزميات للشرطة، وذلك بتنسيق مباشر مع وزارة الدفاع الإسرائيلية. ويُنتج هذا الاندماج البنيوي مسارًا سلسًا بين الابتكار الأكاديمي والتطبيق العسكري، حيث يتحول الفلسطينيون في أراضي 1967 إلى موضوعات غير طوعية لـ»الاختبار الميداني» لهذه الأدوات الرقمية. كما أنّ إدماج المراقبة السيبرانية ضمن مهام الجامعات يحوّل الإنتاج الأكاديمي إلى امتداد للاحتلال بالتحكّم عن بُعد. ومع أنّ التدمير المادي للجامعات الفلسطينية في غزة (الإبادة التعليمية Scholasticide) شكّل محوًا إبستيميًا عميقًا يحتاج إلى دراسة مستقلة موسعة، إلا أنه ينبغي فهمه هنا بوصفه النظير العنيف لصعود الهيمنة الرقمية المُعسكَرة الإسرائيلية.

27 Il Manifesto. (2025, May 31). Fondi europei per la ricerca, 1 miliardo alla difesa di Israele. il Manifesto. [In Italian]. https://ilmanifesto.it/fondi-europei-per-la-ricerca-1-miliardo-alla-difesa-di-israele

28 New Profile. (2025). Academia under orders: Militarism in Israeli academia — The collaboration between Israeli academia, the security establishment, and the military industry. [In Hebrew]. https://drive.google.com/file/d/14ZfAZn-ldt3hQSbtqegNoxE3uLHZoXlS/view

29 ألبانيزي. ف. 2025. من اقتصاد الاحتلال إلى اقتصاد الإبادة: تقرير المقررة الخاصة لوضع حقوق الانسان في الأراضي الفلسطينية المُحتلة منذ العام 1967. الأمم المُتحدة. https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/

30 هاري ديفيز ويوفال أبراهام، «مليون مكالمة في الساعة »: إسرائيل تعتمد على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين»، الجارديان، 6 آب/ أغسطس 2025، https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

31 ديفيز هـ، وأبراهام ي. 23 كانون الثاني/ يناير 2023. كشف: مايكروسوفت تعمق العلاقات مع الجيش الاسرائيلي توّفر تقنية داعمة خلال حرب غزة. ذي جارديان. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft

32 ديفيز هـ. 29 تشرين الأول/ أكتوبر 2025. كشف: اسرائيل طالبت جوجول وأأمازون باستخدام «غمزة» سرية لتجنب الأوامر القانونية. ذي جارديان. https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code

33 سينج ك. 29 آب/ أغسطس 2025. مايكروسوفت تُقيل أربعة عمال احتجوا في الموقع بسبب علاقات الشركة مع اسرائيل. رويترز. https://www.reuters.com/sustainability/society-equity/microsoft-fires-four-workers-on-site-protests-over-companys-ties-israel-2025-08-29/

34 سينج ك. 29 آب/ أغسطس 2025. مايكروسوفت تُقيل أربعة عمال احتجوا في الموقع بسبب علاقات الشركة مع اسرائيل. رويترز. https://www.reuters.com/sustainability/society-equity/microsoft-fires-four-workers-on-site-protests-over-companys-ties-israel-2025-08-29/

35 دي فينك ج. وأودونوفان ك. 16 نيسان/ أبريل 2024. اعتقال موظفي جوجل بعد الاحتجاج على تعاون الشركة مع اسرائيل. واشنطن بوست. https://www.washingtonpost.com/technology/2024/04/16/google-sit-in-employee-protest-nimbus-israel/

36 ميدل ايست آي. 9 أيلول/ سبتمبر 2022. « جوجل تفضل الأبارتهايد على العدل»: احتجاج موظفي مشروع نيمبوس – صفقة اسرائيل، أمازون وجوجل السحابية. Middle East Eye. https://www.middleeasteye.net/news/project-nimbus-israel-apartheid-google-amazon-protests

37 ميدل ايست آي. 18 نيسان/ أبريل 2024. الحرب في غزة: جوجل تُقيل عمالًا احتجوا على العلاقة مع مشروع نيمبوس الاسرائيلي. Middle East Eye. https://www.middleeasteye.net/news/war-gaza-google-fires-employees-protesting-contract-israel-project-nimbus

38 ألبانيزي. ف. 2025. من اقتصاد الاحتلال إلى اقتصاد الإبادة: تقرير المقررة الخاصة لوضع حقوق الانسان في الأراضي الفلسطينية المُحتلة منذ العام 1967. الأمم المُتحدة. https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/

التحكّم التكنولوجي وأنظمة العمل التابعة

تتحقق الإبادة الاقتصادية أيضًا عبر تكريس السيطرة على الأرض، باستخدام التكنولوجيا لتوسيع سيطرة المستوطنين. ويُنظر إلى مشروع Silicon Wadi في القدس الشرقية، من قبل السكان الفلسطينيين، بوصفه أداةً للتهويد تهدف إلى دمج المنطقة في رؤية استيطانية (Al-Arnaout, 2021).[39][40] وفي الوقت نفسه، تُعيد العلاقات الاقتصادية الاستعمارية تشكيل العمل الفلسطيني في صيغ تابعة. إذ تحدّ الأنظمة الإسرائيلية من نمو قطاع تكنولوجيا المعلومات والاتصالات الفلسطيني من خلال قيود الاستيراد وحرمانه من الطيف الترددي. كما أنّ الاستعانة بمصادر خارجية، التي تُقدَّم في خطاب «التعايش»، تستغل الإمكانات العمالية الفلسطينية ورخص كلفتها.[41] وتبقى نماذج التوظيف مثل (NVIDIA) مشروطة بالتصاريح الإسرائيلية والموافقات الأمنية.[42]

وتصف إيناس، وهي من كبار المهندسين، انتظارها اليومي للحصول على تصريح صادر عن الشاباك للوصول إلى مكان عملها في شركة تكنولوجيا في هرتسليا، قائلة: «أحيانًا أنتظر ساعات أو لا أتمكن من العبور أصلًا»، مستحضرة المشهد العبثي الذي تعبر فيه الحاجز حاملةً حاسوبها المحمول، في حين يعبر والدها لبناء المستوطنات. وتجسد هذه الخبرات ما يسميه كلارنو (Clarno, 2018a) الأبارتهايد النيوليبرالي: نظام يستغل العمل الفلسطيني، بينما يحافظ على التبعية من خلال الضبط الإداري وأنظمة الحركة القسرية.

وفي المقابل، يسعى بعض الفلسطينيين إلى ريادة أعمال مستقلة تفاديًا للخضوع. فقد أسّس عدنان شركته الناشئة الخاصة لأنه «لم يُرد أن يكون أسيرًا في نظام استغلالي»، إلا أنّ حتى شراكته العابرة للحدود واجهت عوائق، إذ احتجزته السلطات الإسرائيلية وشريكه التجاري - وهو فلسطيني من أراضي الـ48 - مرارًا على الحواجز، وهو ما فهمه على أنه مصمم من أجل «إبقائنا منقسمين باستمرار». كما يؤكد حازم بالمثل أنّ «أي محاولة لمبادرة فلسطينية مستقلة... توقفها قوات الاحتلال»، بما يبرز رفض إسرائيل السماح باستقلالية تكنولوجية فلسطينية. وتكشف هذه الديناميات أنّ الإبادة الاقتصادية لا تمحو النشاط الاقتصادي الفلسطيني كليًا، بل تعيد تشكيله في صيغ تابعة وقابلة للنكوص، بحيث تحدد السلطة التنظيمية الإسرائيلية إمكانية الوصول إلى الأسواق، والحركة، والنمو. ومنذ 7 أكتوبر 2023، تعمّقت قيود الحركة، وأدّى التدمير العسكري إلى محو قطاع تكنولوجيا المعلومات والاتصالات في غزة، الذي كان يشكل سابقًا 30% من اقتصاد تكنولوجيا المعلومات في الأراضي الفلسطينية المحتلة، بما شمل البنية التحتية والمعرفة.

4.1.3 الإبادة الإبستيمية/المعرفية: المنصات الرقمية ومكان عمل الشركات

تُعدّ المنصات الرقمية ساحات حاسمة للإبادة الإبستيمية/المعرفية، أي التدمير المنهجي للقدرة على إنتاج المعرفة وتداولها. وفي إطار الاستعمار الاستيطاني الرقمي، يتجلّى ذلك بوصفه عنفًا إبستيميًا خوارزميًا يحدّد أيَّ الأصوات تُضخَّم وأيّها يُمحى.

39 المزيد عن هذا المشروع هنا: https://www.jerusalem5800.com/about/the-project

40 المزيد عن هذا المشروع هنا: https://sustainabledevelopment.un.org

41 Alliance for Middle East Peace. (2025, November 20). Working together: Israeli and Palestinian coexistence in tech. https://www.allmep.org/allmep-resources/working-together-israeli-and-palestinian-coexistence-in-tech/

42 تايمز أوف ايسرائيل. 15 تشرين الأول/ أكتوبر 2020. شركة Nvidia الأمريكية توّظف 100 مهندسًا من الضفة الغربية كموظفين مدفوعي الأجر. https://www.timesofisrael.com/us-firm-nvidia-to-employ-100-west-bank-engineers-as-salaried-workers/

يوثّق تقرير حملة (7amleh, 2024)[43] القمعَ المنهجي للمحتوى الفلسطيني من خلال سياسات ضبط منحازة، بما يخلق لاتماثلًا إبستيميًا: فالفلسطينيون مرئيون على نحو مفرط للمراقبة، لكنهم غير مسموعين في الخطاب العام. وقد اشتدّ هذا النمط بعد 7 أكتوبر. فقد عمدت منصات Meta إلى تضخيم العنف ونزع الإنسانية باللغة العبرية (مثل وصف الفلسطينيين بـ»الحيوانات البشرية»)، ما أتاح تداول التحريض، في الوقت الذي كانت تمارس فيه رقابة منهجية على السرديات الفلسطينية.[44][45] كما شغّل الجيش الإسرائيلي نفسه قناة على Telegram لنشر محتوى صادم ولغة تجريد من الإنسانية، بما يؤكد أن التحريض كان صادرًا عن الجيش الإسرائيلي نفسه.[46] ويكشف هذا التفاوت عن معيار مزدوج متجذر في سياسات Meta، حيث إنّ التساهل مع التحريض بالعبرية يرقى إلى مستوى التواطؤ.[47]

وتمتد الإزالة الإبستيمية إلى الفضاءات «الحيادية» في أماكن العمل التكنولوجية. فالقمع الرقمي ينعكس في مراكز التكنولوجيا، حيث يُسكت المهندسون الفلسطينيون أو يُفصلون من أعمالهم.[48][49] وتوثّق دراسة استقصائية أجرتها NAS[50] وجود حالة خوف واسعة بين المهندسين الفلسطينيين في إسرائيل - إذ أفاد 44% منهم بأنهم يخشون الذهاب إلى العمل - بما يبرز كيف يعيد مكان العمل إنتاج الشك المجتمعي ويفشل في احترام التنوع في زمن الأزمات.[51] ويُنتج ذلك بيئة معرفية عدائية، يجد فيها المهني الفلسطيني نفسه مضطرًا إلى الاختيار بين مساره المهني وواقعه.

وفوق ذلك، جرى إسكات الخطاب نفسه حول التنوع. فبينما دأبت شركات التكنولوجيا الدولية العاملة في إسرائيل على تسويق نفسها عالميًا من خلال خطاب «التعايش» و»الشمول»، كشفت الوقائع التي تلت 7 أكتوبر هشاشة هذه الأطر وسطحيّتها. فالتنوع مقبول فقط ما دام «صامتًا سياسيًا». وينعكس هذا الفهم الملتبس أيضًا في الأوساط التكنولوجية «التقدمية» الأمريكية والإسرائيلية، التي تبنّت الموقف المعروف باسم "Progressive Except for Palestine" (PEP)، كما صاغه غسان الحاج (Al-Hajj, 2019).

وفي هذا الإطار، يعمل مكان العمل في قطاع التكنولوجيا بوصفه حدودًا ثانوية، حيث

43 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 28 آب/ أغسطس 2024. 70% من الشباب الفلسطينيّ في الداخل يمارسون الرقابة الذاتيّة على شبكة الإنترنت https://7amleh.org/post/palestinian-youth-practice-self-censorship-online-ar

44 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 2 ايلول/ سبتمبر 2025. دور «ميتا» في تضخيم المحتوى الضار ضد الفلسطينيّين خلال حرب الإبادة في غزة. https://7amleh.org/post/meta-s-role-during-genocide-ar

45 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 28 آب/ أغسطس 2024. 70% من الشباب الفلسطينيّ في الداخل يمارسون الرقابة الذاتيّة على شبكة الإنترنت https://7amleh.org/post/palestinian-youth-practice-self-censorship-online-ar

46 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 2 ايلول/ سبتمبر 2025. دور «ميتا» في تضخيم المحتوى الضار ضد الفلسطينيّين خلال حرب الإبادة في غزة. https://7amleh.org/post/meta-s-role-during-genocide-ar

47 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 2 ايلول/ سبتمبر 2025. دور «ميتا» في تضخيم المحتوى الضار ضد الفلسطينيّين خلال حرب الإبادة في غزة. https://7amleh.org/post/meta-s-role-during-genocide-ar

48 7amleh – The Arab Center for the Advancement of Social Media. (2024). Delete the Issue: Tech Worker Testimonies on Palestinian Advocacy and Workplace Suppression [PDF report]. https://7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf

49 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 2 ايلول/ سبتمبر 2025. دور «ميتا» في تضخيم المحتوى الضار ضد الفلسطينيّين خلال حرب الإبادة في غزة. https://7amleh.org/post/meta-s-role-during-genocide-ar

50 NAS Research & Consulting. (2024, January). Arabs in Hi-Tech: From Diversity to Inclusion [PDF report]. https://www.nasconsulting.co.il/wp-content/uploads/2024/01/NAS_Arabs-in-Hi-Tech-Diversity-to-Inclusion_En_Tsofen_Aug23.pdf

51 Gams, N. (2024, January 22). "It's hard to say what would be different if I were Israeli, but I come from a country ..." TheMarker. [In Hebrew]. https://www.themarker.com/career/2024-01-22/ty-article-magazine/.premium/0000018d-2bf2-daf5-a1bf-aff282150000

يُفرَض على العامل الفلسطيني «المثالي» أن يكون منزوع السياسة وغير مرئي.

4.2 مقاومة الإبادة: الصمود الرقمي بوصفه بنية متعددة الطبقات للحضور والنجاة/البقاء والمستقبل

يتجسّد الصمود الرقمي من خلال البنى التحتية المضادّة، والأرشيفات، والشبكات البديلة التي تقاوم الإبادة الجسدية والاقتصادية والإبستيمية/المعرفية. فالقصف، والحصار، والتهجير، والتجويع، وانهيار البنى التحتية، والتشابك مع الشركات، والرقابة، والإبادة التعليمية، ليست عمليات منفصلة، بل آليات متداخلة يعزّز بعضها بعضًا، صُمّمت لإنتاج الإقصاء والمحو. وفي مواجهة ذلك، يبرز الصمود الرقمي بوصفه بنيةَ مقاومةٍ متعدّدة الطبقات تُسهم في صون الحياة الفلسطينية، وحاضرها ومستقبلها عبر هذه المجالات كافة. ولا يتخذ الصمود الرقمي شكلَ أفعالٍ فردية معزولة على الإنترنت، بل يتجسّد عبر أربع ممارسات مترابطة: الاستمرار المادي والبنيوي، والاتصال بوصفه فعلَ رعايةٍ وبقاء، والشهادة الرقمية، والأرشيفات المضادّة والحشد المؤسسي، وإعادة بناء الوطن بوصفها فعلًا من أفعال الصمود الرقمي والتوجّه نحو المستقبل.

4.2.1 الاتصال والمثابرة البنيوية

تُظهر الأدلة الميدانية أن الفلسطينيين يستجيبون للإبادة المادية - من قصف وتهجير وحصار وانقطاعات اتصالات مُفتعلة - عبر بناء بنى تحتية مرتجلة تحافظ على الحياة، والاتصال، والحضور. فقد حشد متطوعون من الشتات، ومنظمات للحقوق الرقمية، ومدنيون، أدوات مثل الشرائح الإلكترونية eSIMs، والشبكات الخاصة الافتراضية VPNs، والشبكات المتداخلة mesh networks، والروابط الفضائية، والحسابات الموازية، لمواجهة الفصل المتعمّد عن العالم. وتُظهر النتائج أنّ البنية التحتية الرقمية لا تُعامَل هنا بوصفها أداةَ تواصلٍ ثانوية، بل بوصفها بنيةً للبقاء. فالبقاء على اتصال ليس فعلًا رمزيًا، بل مسألةٌ وجودية. وتؤطّر حملات مثل #ConnectingGaza[52] وReconnect Gaza[53] الاتصالَ لا بوصفه حقًّا في التواصل فحسب، بل بوصفه شرطًا من شروط النجاة، بما ينسجم مع أدبيات التصميم المُناهِض للاستعمار، التي تصبح فيها الممارسة البنيوية وسيلةً لإعادة توظيف التكنولوجيا في سبيل التحرر.

وخلال فترات انقطاع الاتصالات، يغدو الحفاظ على الاتصال الرقمي فعلًا يؤكد الحياة. كما دعمت مجموعات من المهندسين الشعبيين والمنظمات غير الحكومية - مثل APC (Association for Progressive Communications) وائتلاف KeepItOn التابع لـ Access Now - الشبكاتِ المتداخلة، والاتصالات الفضائية، وأنظمة الأرشفة غير المتصلة بالشبكة، حفاظًا على تدفق المعلومات. وتوسّع هذه الأفعال القائمة على الرعاية التكنولوجية معنى الصمود، بحيث لا يعود مقتصرًا على التحدّي، بل يشمل أيضًا صيانة العلاقات وتبادل العون المتبادل. وفي هذا السياق، يدلّ الصمود الرقمي على الممارسة الأخلاقية المتمثلة في «البقاء على الشبكة» بوصفها رفضًا جماعيًا للمحو.

52 Landy, H., & Shabana, Y. (2025, October –). Tens of thousands of Palestinians in Gaza are staying connected to the world via donated eSIMs. Quartz. https://qz.com/tens-of-thousands-of-palestinians-in-gaza-are-staying-c-1851078107

53 حملة – المركز العربي لتطوير الإعلام الاجتماعي. 22 آب/ أغسطس 2025. #ReconnectGaza – Reconnecting Gaza, empowering the future. https://7amleh.org/reconnectgaza/en

وتُغني السرديات الفردية هذه الصورة، إذ تُظهر كيف يتعذّر فصل النجاة الرقمية عن النجاة الجسدية. فقد وصفت ياسمينا، وهي عاملة فلسطينية في قطاع التكنولوجيا في غزة، استشهدت لاحقًا في غارات عام 2024، كيف أدّت أزمات الكهرباء والإنترنت إلى تعطيل عملها مرارًا. وفي ظل القصف، ابتكرت سبلًا للاستمرار، فقالت: "لم تكن الكهرباء تكاد تتوفر... وكان والدي يساعدني عبر شحن الحاسوب المحمول في المسجد، لأنه المكان الوحيد الذي كان فيه مولّد كهرباء دائم... وكان يفعل ذلك خمس مرات يوميًا، مع كل صلاة من الصلوات الخمس».

يكشف هذا السرد أنّ النجاة الرقمية كانت جهدًا عائليًا جماعيًا، قوامه الرعاية والتحمّل. فمولّد المسجد الذي أُعدّ أصلًا للعبادة صار جزءًا من شبكة مرتجلة التقت فيها المساحة الدينية، والعمل الأسري، والحاجة التكنولوجية. ولم ينبع الاتصال هنا من بنية تحتية رسمية، بل من تنسيق علاقاتي وتضحية يومية. وفي هذا السياق، لم يكن البقاء على الشبكة مجرد مهمة تقنية، بل فعلًا من أفعال البقاء والظهور. فقد ارتبط استمرار حضور ياسمينا برعاية تمتد بين الأجيال والإبقاء المتعمد للاتصال. وهكذا، تجسّد الصمود الرقمي في ممارسات يومية من التحمّل.

ولا يقتصر هذا الاتصال على حدود المنزل، بل يمتد إلى شبكات عابرة للحدود. ففي ظل انعدام أمن غذائي حاد في غزة[54] - وثّقته منظمة الأغذية والزراعة (FAO)[55] وبرنامج الأغذية العالمي (WFP)[56] - أصبحت المنصات الرقمية قنواتٍ للبقاء، وبرزت عبرها أشكال من التضامن الشعبي. فعلى سبيل المثال، استخدمت الطاهية الأردنية ياسمين نصر[57] منصة إنستغرام لتبادل طرق إعداد وجبات من مكونات شحيحة. ويُظهر هذا النشاط التضامني كيف تتيح المنصات الرقمية أشكالًا من التضامن العلاقاتي العابر للحدود، على نحو ينسجم مع الأدبيات التي تناولت الأبعاد الوجدانية للانخراط الرقمي.

وتُبيّن هذه التبادلات أنّ الاتصال يعمل بوصفه رعاية ممتدة عبر الحدود. فمن خلال التضامنات الوجدانية والعملية، تتحول المنصات الرقمية إلى بنى تحتية للعون المتبادل. فالقدرة على الاتصال تتيح تجسيد الطمأنينة العاطفية، وتبادل المعلومات، واستراتيجيات البقاء المادي، رغم القيود المفروضة على المكان والحركة.

وعليه، يتجاوز الصمود الرقمي معنى التحدّي ليشمل الاتصال بوصفه ممارسةً مقصودةً للرعاية والبقاء. فـ«البقاء على الشبكة» هو رفضٌ للموت الاجتماعي، وإصرارٌ على استمرارية العلاقة حتى حين تُدمَّر البنى التحتية المادية. وبذلك يصبح الاتصال، في آنٍ واحد، شريانَ حياةٍ وفعلًا سياسيًا، ممارسةً يوميةً للحضور في مواجهة الغياب.

54 منظمة الصحة العالمية. 22 آب/ أغسطس 2025. تأكيد المجاعة في غزة لأول مرة. https://www.who.int/news/item/22-08-2025-famine-confirmed-for-first-time-in-gaza?utm_source

55 The Food and Agriculture Organization

56 The World Food Programme

57 راجع حساب ياسمين على الانستغرام: https://www.instagram.com/yasmin.nasir

4.2.2 الشهادة الرقمية، والأرشيفات المضادّة، والتعبئة المؤسسية

يتتبّع هذا المحور كيف يوظّف الفلسطينيون الأدوات الرقمية بوصفها استراتيجيةً متعددة الأبعاد في مواجهة الإبادة الجسدية والإبستيمية/المعرفية. فمن خلال الشهادة الفورية، والأرشفة المضادّة، والمناصرة المؤسسية، يصبح الفضاء الرقمي ليس فقط ساحةً للمراقبة، بل أيضًا مجالًا للصمود، ولسيادة السرد، ولاستمرارية التاريخ.

الشهادة الرقمية بوصفها مقاومة

تُظهر الشهادة الرقمية والتوثيق اللذان ينجزهما صحفيون مثل معتز عزايزة[58] وبيسان عودة[59] (الصورتان 1 و2) كيف يصبح الحضور شكلًا من أشكال المقاومة. فمن قلب غزة، وفي ظل خطر بالغ، يقومان بالبث المباشر، والتصوير، وأرشفة الأحداث في الزمن الحقيقي، بما يتحدى في آنٍ واحد القيود المفروضة على الإعلام الأجنبي وممارسات ضبط المحتوى التي تنتهجها المنصات. وهنا يغدو التوثيق فعلًا سياسيًا: إذ ينازع احتكار السرد، ويُنتج سجلًا إثباتيًا بديلًا. وبذلك تصبح حالة الحضور بحد ذاتها فعلًا من أفعال المقاومة الإلكترونية (Khoury-Machool, 2007; Shehadeh, 2023).

الصورة 1

الصورة 2

58 مُعتز عزايزة – صحافي ومصوّر حاصل على شهادة بالترجمة الانجليزية من جامعة الأزهر وأهي إحدى الجامعات التي دمرتها إسرائيل مؤخرًا في قصف جويّ – يظهر كأحد أكثر السرديين تأثيرًا في هذه الحرب. بدأ مسيرته المهنية كمصوّر مستقل، وأصبح عزايزة أحد أكثر الشخصيات متابعة والأصوات الأكثر موثوقية التي تجلب التقارير من غزة أثناء العدوان العسكري الاسرائيلي على غزة الذي انطلق في السابع من أكتوبر. واختارت مجلة «تايم» إحدى صوره، التي تصوّر طفلًا تحت الحطام والدمار الذي تسبب به القصف الاسرائيلي، كإحدى الصور التي تمثّل العام 2024 (راجعوا الرابط: https://www.arabnews.com/node/2612324/amp?utm_source)

59 بيسان – صانعة مُحتوى رقمي وناشطة شابة من غزة حاصلة على درجة في الاقتصاد والأعمال، حصلت على اعتراف دوليّ لتقاريرها الميدانية. بواسطة سلسلة الإعلام الرقمي "This is Bisan from Gaza" و "I'm Still Alive"، وثّقت حياتها اليومية تحت القصف بمتنوّع من الوضوح السرديّ الفوريّ يصل لملايين البشر. حظيت لعملها باعتراف دوليّ، وفازت بتسمية في جائزة الايمي تحت فئة Outstanding Hard News Feature Story: Short Form at the 2024 News and Documentary Emmy Awards.

التضامن الرقمي والبقاء

إلى جانب القصف، يشكّل التجويع بُعدًا آخر من أبعاد الإزالة. فقد أفادت هيئات مثل منظمة الأغذية والزراعة (FAO)[60] وبرنامج الأغذية العالمي (WFP)[61] ببلوغ مستويات غير مسبوقة من انعدام الأمن الغذائي الحاد في غزة.[62] وفي مواجهة ذلك، برزت أشكال من التضامن العابر للحدود عبر الفضاء الرقمي. فقد استخدمت الشيف الأردنية ياسمين نصر منصة إنستغرام لتبادل طرق طبخ مرتجلة، مقدّمةً معرفة عملية ودعمًا رمزيًا في آنٍ معًا[63]. وبذلك، لا تعمل وسائل التواصل الاجتماعي مجرد قناة لنقل المعلومات، بل تصبح أيضًا فضاءً للرعاية العلاقية، تُسهم في صون الحياة من خلال المعرفة المتبادلة.

الأرشيفات المضادّة والعصيان الإبستيمي/المعرفي

في مواجهة الرقابة والتدمير، اتجه الفلسطينيون على نحو متزايد إلى الحفاظ على الحضور الرقمي (Ghaddar, 2025). وكما تشير إحدى الباحثات/أحد الباحثين، فإنّ «هذا المحو المنهجي ليس جديدًا».[64] وانطلاقًا من ذلك، تؤكد مبادرات مثل الأرشيف الرقمي للمتحف الفلسطيني وDecolonize Palestine مشروعيةَ المنظور الفلسطيني وسلطته المعرفية، رافضةً السيطرة الاستعمارية على ما يُعتَبر معرفةً مشروعة. كما تنتشر على نطاق واسع الأرشيفات الصغرى - من تسجيل وتوثيق، والتقاط صور، والمشاركة الرقمية - خلال فترات انقطاع الاتصال، في حين تنسّق مشاريع مثل Fighting Erasure جهودًا عابرة للحدود من أجل الحفظ والصون. وتشكّل هذه الممارسات، مجتمعةً، بنيةً تحتية للذاكرة وللعصيان الإبستيمي/المعرفي، بما يحفظ الاستمرارية التاريخية ويُنازع التراتبيات المعرفية (Mignolo, 2009, 2011).

المساءلة المؤسسية ومساءلة الشركات

يعمل الصمود الرقمي أيضًا من خلال مناصرة منظّمة تقودها مؤسسات المجتمع المدني. فتقوم منظمات مثل حملة وعدالة ومركز صدى سوشال وSMEX بتوثيق التحيّز الخوارزمي وحذف المحتوى، محوّلةً الحالات الفردية إلى أدلة على وجود رقابة بنيوية. وقد دفعت حملة Facebook, We Need to Talk[65] إلى إجراء تدقيق مستقل من قبل Business for Social Responsibility، أكّد وجود تفاوتات منهجية في سياسات الإشراف على المحتوى.[66]

وتمتدّ التعبئة الموازية إلى المجال الأكاديمي وقطاع التكنولوجيا. إذ تتحدى حركة المقاطعة وسحب الاستثمارات وفرض العقوبات (BDS)[67] والحملة الفلسطينية

60 The Food and Agriculture Organization

61 The World Food Programme

62 منظمة الصحة العالمية. 22 آب/ أغسطس 2025. تأكيد المجاعة في غزة لأول مرة. https://www.who.int/news/item/22-08-2025-famine-confirmed-for-first-time-in-gaza?utm_source

63 راجع حساب ياسمين على الانستغرام: https://www.instagram.com/yasmin.nasir

64 ويلسون، ل. 27 حزيران/ يونيو 2025. إبادة التاريخ في غزة: تدمير اسرائيل للأرشيفات الرسمية والخاصة يغيّر شكل مسرد قصة فلسطين. مجلة نيو لاينز. https://newlinesmag.com/essays/historicide-in-gaza/

65 **حملة – المركز العربي لتطوير الإعلام الاجتماعي. بدون تاريخ.** Delete the issue (Issue 11.11). https://www.7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf

66 Human Rights Watch. (2022, September 27). Statement Regarding BSR's HRA for Meta on Palestine & Israel. https://www.hrw.org/news/2022/09/27/statement-regarding-bsrs-hra-meta-palestine-israel

67 BDS Movement. (n.d.). Academic Boycott. https://bdsmovement.net/academic-boycott

للمقاطعة الأكاديمية والثقافية لإسرائيل (PACBI)[68] الروابطَ التي تجمع الجامعات والشركات بالبنى التحتية العسكرية والرقابية الإسرائيلية.[69] وترى PACBI أنّ المقاطعة تُعطّل مسارات إنتاج المعرفة التي تغذّي الأنظمة العسكرية وأنظمة المراقبة. كما أنّ تصاعد النشاط الطلابي العالمي بعد 7 أكتوبر كشف ما وُصف بـ «نفاق» الجامعات المرموقة، الأمر الذي دفع المؤسس المشارك لحركة المقاطعة عمر البرغوثي إلى توصيف هذه اللحظة بأنها «لحظة فلسطين الجنوب أفريقية».[70] وقد أفضى هذا الزخم إلى تبنّي عشرات الجامعات سياسات سحب استثمارات أو تعليق شراكات، بما يمثّل انخراطًا أكاديميًا عالميًا غير مسبوق.

وداخل شركات التكنولوجيا العالمية، تعارض ائتلافات مثل No Tech for Apartheid مشاريع مثل مشروع Project Nimbus[71] (انظر الصورة 3)، وهو عقد للحوسبة السحابية بين غوغل وأمازون والحكومة الإسرائيلية.[72] كما تستهدف حملات العمل المباشر، مثل Shut Elbit Down[73] (انظر الصورة 4)، الشركاتِ المتورطة في تقنيات المراقبة، والتحليلات التنبؤية، والبنى التحتية السحابية. وتشكل هذه المبادرات مجتمعةً عدّةً للمقاومة الاقتصادية والإبستيمية/المعرفية، إذ تكشف تواطؤ الشركات وتنازع السلطة الاستعمارية الرقمية من داخل بنياتها التحتية نفسها.

الصورة 4

الصورة 3

4.2.3 إعادة بناء الأمة كفعلٍ من أفعال الصمود الرقمي والتوجّه نحو المستقبل

يُؤطِّر هذا المحور بناءَ الأمة في ظلّ الحصار لا بوصفه مجرد تطلّع ما بعد استعماري، بل باعتباره ممارسةً مستمرةً من الصمود، موجَّهةً نحو المستقبل ونحو بناء الأمة اقتصاديًا. وتُظهر المبادرات الفلسطينية في مجال التكنولوجيا وريادة الأعمال أن إعادة البناء لا تقتصر على الإعمار المادي، بل تشمل أيضًا إنشاءَ منظومات تكنولوجية اقتصادية ومعرفية وبنيوية بديلة، افتراضيًا وماديًا. وبهذا المعنى، تصبح الممارسة التكنولوجية، في آنٍ واحد، استراتيجيةً للبقاء وفعلًا سياسيًا استباقيًا ـ أي محاولةً لتجسيد الاستقلالية داخل بُنى القيد.

68 The Palestinian Campaign for the Academic and Cultural Boycott of Israel

69 حركة المقاطعة. لا تاريخ. المقاطعة الأكاديمية.. https://bdsmovement.net/academic-boycott

70 ذي جارديان. 4 حزيران/ يونيو 2024. مؤسس حملة المقاطعة يشيد بالمظاهرات في الجامعات وجعل سحب الاستثمارات من اسرائيل أمرًا شائعًا.. https://www.theguardian.com/us-news/article/2024/jun/04/bds-omar-barghouti-israel-campus-protests

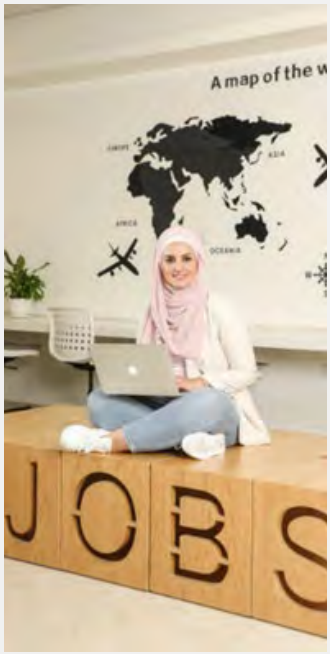
71 ميدل ايست آي. 2 أيلول/ سبتمبر 2022. مشروع نيمبوس: موظف جوجل يتهم عملاق التكنولوجيا بكسب الأرباح والانتفاع من المعاناة الفلسطينية. Middle East Eye. https://www.middleeasteye.net/news/palestine-google-project-nimbus-employee-accuses-profiteering-pain

72 ذي جارديان. 19 آب/ أغسطس 2025. موظفو مايكروسوفت يحتجون على صفقة التكنولوجيا بين واشنطن واسرائيل. https://www.theguardian.com/technology/2025/aug/19/microsoft-workers-protest-washington-israel

73 ذي جارديان. 19 آب/ أغسطس 2025. موظفو مايكروسوفت يحتجون على صفقة التكنولوجيا بين واشنطن واسرائيل. https://www.theguardian.com/technology/2025/aug/19/microsoft-workers-protest-washington-israel

بناء المنظومات البديلة

تشكل المبادرات التكنولوجية الفلسطينية قوة مؤسساتية موازنة للاعتماد البنيوي. فGaza Sky Geeks (حاضنة رقمية) وMENA Alliances (التي أسستها عبير أبو غيث - انظر الصورة 6 أدناه) تربطان العاملين بالأسواق العالمية، متجاوزتين قيود الحركة ومخفِّضتين الاعتماد على سوق العمل الإسرائيلي. كما يعيد Palestine Open Maps بناء الجغرافيات الممحوة، فيما يعزّز BuildPalestine الابتكارَ المجتمعي القائم على المجتمع المحلي. وتُسهم هذه المبادرات في بناء منظومات اقتصادية مستدامة ومستقلة (Althalathini et al., 2020; Althalathini & Tlaiss, 2023; Aouragh, 2011; Rindova et al., 2009)، مجسِّدةً الفاعلية الريادية والممارسة التكنولوجية المناهضة للاستعمار، رغم واقع الاستعمار الاستيطاني.



الصورة ٦

وقد لخّصت عبير، وهي رائدة أعمال في مجال التكنولوجيا من جنين، هذا المنطق بوضوح. فعلى الرغم من قيود الحركة وغياب المطار، شدّدت على قابلية العمل الرقمي للنقل وعلى الاستقلالية التي يتيحها:

"اللاب توب مهم جدًا؛ وكنت دائمًا أقول لوالديّ ولأختي اللذين يعملان إن أهم شيء هو اللاب توب. وحتى لو أُغلِقت كل الطرق في وجهك، فإن اللاب توب يظل بوابتك إلى العالم... لقد كان الشيء الوحيد الذي أحتاجه للتواصل مع الناس وتوظيف أشخاص من غزة للعمل معي".

تُبرز شهادة عبير كيف يُحوّل العمل الرقمي التقييدَ المكاني إلى حركة عبر الشبكة. ويعمل الحاسوب المحمول بوصفه بنيةً تحتيةً مصغّرة للاستقلالية، بما يتيح المشاركة في الأسواق العالمية رغم الإغلاق الجغرافي وقيود الحركة. وهكذا لا تؤدي الاتصالية وظيفةً اقتصاديةً فحسب، بل تضطلع أيضًا بدور سياسي يتحدّى فرضَ الشلل الحركي. ومن خلال توظيف عاملين من غزة، تُظهر عبير كذلك كيف تعيد المنصات الرقمية وصلَ الجغرافيات الفلسطينية المجزّأة، بما يعزّز التماسك الاقتصادي الداخلي. وانسجامًا مع الأدبيات المتعلقة بالفاعلية الريادية والعبر-وطنية الرقمية (Aouragh, 2011; Rindova et al., 2009)، تضع مثل هذه المبادرات التكنولوجيا في موقع البنية التحتية للصمود - أي وسيلة لإعادة تنظيم العلاقات الاقتصادية بصورة فاعلة تحت شروط التقييد، بدلا من تحملها فقط.

مجد، وهي رائدة أعمال أخرى في مجال التكنولوجيا من غزة، تُجسّد شكلًا متجذرًا ماديًا من الصمود الرقمي. وانطلاقًا من خبرتها التقنية، أسست SunBox، وهي شركة ناشئة في مجال الطاقة الشمسية وفّرت الكهرباء المستدامة وإمكانية الوصول إلى المياه لعشرات الآلاف من السكان، بمن فيهم الفئات الهشّة، من دون الحاجة إلى إسرائيل. وقالت: "بالكاد تتوفر لدينا الكهرباء؛ فقبل السابع من أكتوبر كنا نحصل على الكهرباء لمدة 6 ساعات فقط. ومن هنا جاءت فكرة SunBox"

وفي سياق الانهيار البنيوي المزمن ونقص الطاقة المستمر، أدّت التكنولوجيا المتجددة وظيفةً مزدوجة، باعتبارها آليةً للبقاء ونموذجًا للاستقلالية اللامركزية في الوقت نفسه.

الصورة 7

وبعد أن دمّرت غارة جوية منزلها، قامت مجد ووالدها بتطوير GreenCake، وهي مبادرة حوّلت ركام المباني المدمرة إلى مواد بناء مُعاد تدويرها. وقد أكسبها هذا المشروع لقب "بنت الحجر" (The Brick Lady) (انظر الصورة 7). ويُظهر مسارها كيف يمكن تعبئة المهارة التكنولوجية لإعادة بناء كلٍّ من الظروف المادية والبنية الاجتماعية في ظل الهشاشة القصوى. وقد شاركت قائلة:

"قُتل أصدقائي خلال إحدى الاجتياحات العسكرية... وكان لهذا الحادث أثر كبير جدًا؛ كما دُمّر منزلنا أيضًا. وشعرتُ بحالة من الإحباط، وإلى متى سننتظر قطر والأمم المتحدة لكي تعيدا بناء بلدتنا؟ وإلى متى سننتظر مساعدة المنظمات الدولية، في حين أن أربعةً وتسعين بالمئة منا متعلمون؟ فلماذا لا نُنتج؟ لقد كان هذا الفضول موجودًا لديّ دائمًا؛ فأنت ترى الناس في الخارج يُنتجون، فلماذا لا نُنتج نحن أيضًا؟"

غير أنّ الحرب على غزة عطّلت هذه المشاريع بصورة بالغة. فقد دُفنت SunBox تحت الأنقاض. وكتبت مجد على صفحتها في فيسبوك (انظر الصورة 8):

"كل الذكريات، والشهادات، والجوائز، والهدايا، والصور، أي كل ثمرة حياتي العملية، اختفت وسحقت تحت الأنقاض."

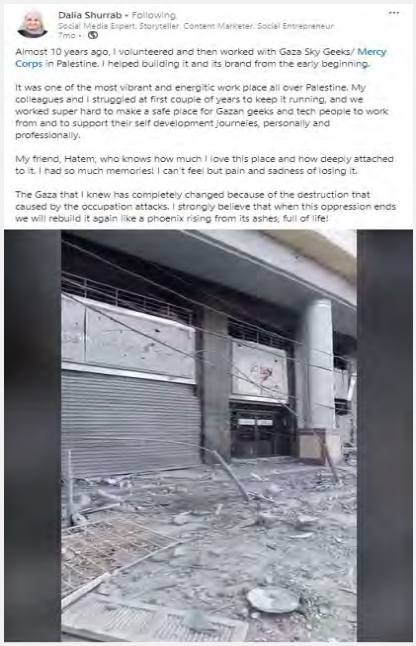
ولا يعكس هذا التصريح الدمار المادي فحسب، بل أيضًا الفقدان المعرفي، أي محو المسارات المهنية وما راكمته من اعتراف وتقدير.

الصورة 8

وبالمثل، نشرت داليا، وهي رائدة أعمال أخرى في مجال التكنولوجيا من غزة، صورةً للمقر المتضرر لـ Gaza Sky Geeks كما هو موضّح أدناه (انظر الصورة 9). وتحت صورة الأنقاض، كتبت:

"لقد تغيّرت غزة التي عرفتها بالكامل بفعل الدمار الذي تسببت به هجمات الاحتلال. وأؤمن من كل قلبي أننا سنعيد بناءها كطائر الفينيق الذي ينهض من الرماد وهي مفعمةً بالحياة!"

تكشف هذه الشهادات كيف تتوسط المنصات الرقمية بين الدمار والتطلّع إلى المستقبل في آنٍ واحد، فتصبح منصات التواصل الاجتماعي فضاءً يُوثَّق فيه الفقد، ويُعبَّر فيه عن الحزن، ويُتخيَّل فيه إعادة الإعمار. وهكذا تتحول المرونة الفردية إلى مقاومة تواصلية: تأكيدٌ على الحضور، والاستمرارية، والعزم الجماعي. وتتقاطع مثل هذه الحالات مع الأدبيات التي تشير إلى أن ريادة الأعمال التكنولوجية يمكن أن تشكّل مسارًا تحرريًا للمجتمعات المهمّشة الساعية إلى الاستقلالية والتحول الجماعي (Awwad & Toyama, 2024; Mignolo, 2009; Rindova et al., 2009; Shehadeh, 2023). وفي هذا التصور، لا يكون الابتكار التكنولوجي منفصلًا عن السياسة، بل متجذرًا في صراعات البقاء والكرامة وصناعة المستقبل.



الصورة 9

وفي الختام، فإن إعادة البناء عبر التكنولوجيا والمنصات الرقمية لا تُرجأ إلى مستقبل افتراضي لما بعد الحرب، بل تتكشف وسط الدمار ذاته بوصفها فعلًا من أفعال الصمود وادعاءً بحقّ التوجّه نحو المستقبل. فمن خلال المنظومات الرقمية البديلة، ومبادرات الطاقة المتجددة، وإعادة الإعمار الريادية، والشهادة عبر الإنترنت، يُجسّد الفلسطينيون شكلًا من أشكال بناء الأمة قائمًا على المهارة التكنولوجية والمخيلة الجماعية. وتُظهر هذه الممارسات أن التكنولوجيا يمكن أن تكون، ليس فقط أداةً للسيطرة، بل أيضًا وسيطًا للبقاء، وإعادة الإعمار، والفاعلية السياسية. وهكذا تبرز إعادة بناء غزة باعتبارها مشروعًا ماديًا ومعرفيًا، في آنٍ واحد، مشروعًا يُصرّ على الحياة، والاستمرارية، والحق في تخيّل مستقبل أفضل.

الخلاصات

تُظهر هذه الدراسة أن الاحتلال الإسرائيلي دخل مرحلةً رقميةً مكتملة، تؤدي فيها الأنظمة الخوارزمية، والبنى التحتية للبيانات، واقتصادات الابتكار، وظائفَ كانت تُمارَس سابقًا بواسطة الجنود والبيروقراطيين. فالحوكمة بالتحكم عن بُعد - من خلال الاستهداف المدعوم بالذكاء الاصطناعي، والمراقبة البيومترية، والحواجز المؤتمتة، والتحكم بالشبكات - لا تستبدل الهيمنة الاستعمارية، بل تُكثّفها. ويغدو الفلسطينيون مجرد موضوع بيانات لا تعار أي أهمية ويفقدوا قدرتهم على الفعل السياسي؛ أي يصبح حضورهم محصور على المعدات التكنولوجية التي يوظفها الاحتلال دون الحضور في الخطابات الإنسانية والأكاديمية وخطابات الابتكار. هذا هو أتمتة الأبارتهايد: ترجمة الحوكمة المُعنصَرة إلى صيغة الكترونية.

ويحدد التحليل ثلاثة أنماط مترابطة من الإبادة الرقمية: النمط المادي (الاستهداف المؤتمت وأنظمة مثل Blue Wolf وLavender)، والنمط الاقتصادي (إدماج الاحتلال في الأسواق العالمية وحرمان الفلسطينيين من السيادة التكنولوجية عبر الترابط المدني–العسكري–الأكاديمي)، والنمط المعرفي (رقابة المنصات، وتدمير الأرشيف، والإبادة التعليمية/الأكاديمية). وفي مواجهة هذا النظام، يطوّر الفلسطينيون الصمود الرقمي بوصفه شكلًا من أشكال العصيان المعرفي، الذي يبني بنى تحتية بديلة للتواصل، والأرشفة، والمجتمع. ومن خلال التوثيق الموزّع والتضامن العابر للحدود الوطنية، يستعيدون الفضاء الرقمي بوصفه ساحةً للمقاومة والصمود.

إن مقاومة الاحتلال الخوارزمي تتطلب تفكيك الأنظمة الرقمية القمعية وتصميمَ آفاقٍ تكنولوجيةٍ تحرريةٍ مناهضةٍ للاستعمار، تُعطي الأولوية للسيادة الرقمية الفلسطينية، متجاوزةً الأطر الغربية الضيقة لأخلاقيات الذكاء الاصطناعي. ويؤكد صعود الصمود الرقمي أن الصراعات حول البيانات والذكاء الاصطناعي تُعد جزءًا لا يتجزأ من النضال من أجل التحرر والمساءلة.

المراجع

- 7amleh. (2024). Delete the issue-11.11 Tech Worker Testimonies on Palestinian Advocacy & Workplace suppression. https://7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf
- Abu-Lughod, L. (2020). Imagining Palestine's Alter-Natives: Settler Colonialism and Museum Politics. Critical Inquiry, (47), 1–27.
- Ahmad, R. S. (2021). The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. In 7amleh –The Arab Center for Social Media Advancement The.
- Al-Arnaout, A. al-R. (2021). A " Silicon " Disaster Threatening Wadi al-Jawz. Jerusalem Quarterly, (85), 125–131. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.palestine-studies.org/sites/default/files/jq-articles/A%20%E2%80%9CSilicon%E2%80%9D%20Disaster%20Threatening%20Wadi%20al-Joz.pdf
- Albanese, F. (2025). From economy of occupation to economy of genocide (A/HRC/5923/). https://www.un.org/unispal/document/a-hrc-5923--from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/
- Al-Hajj, G. (2019). Palestine and the West: Colonialism and the Lack of Belonging. Majallat al-Dirasat al-Filastiniyya, Institute for Palestine Studies, Summer 2019(119). https://www.palestine-studies.org/en/node/235542
- Al-Salhi, A. (2021). The Palestinian Public's Perception of Palestinian CSOs. In 7amleh - The Arab Center for the Advancement of Social Media (Number October).
- Althalathini, D., Al-Dajani, H., & Apostolopoulos, N. (2020). Navigating Gaza's Conflict through Women's Entrepreneurship. Journal of Small Business Management, 58(4), 678–695.
- Althalathini, D., & Tlaiss, H. A. (2023). Of resistance to patriarchy and occupation through a virtual bazaar: an institutional theory critique of the emancipatory potential of Palestinian women's digital entrepreneurship. Entrepreneurship and Regional Development. https://doi.org/10.108008985626.2023.2241412/
- Amit, G. (2011). Salvage or Plunder? Israel's "Collection" of Private Palestinian Libraries in West Jerusalem. Journal of Palestine Studies, 40(4), 6–23. https://www.palestine-studies.org/en/node/42473
- Aouragh, M. (2011). Palestine online: Transnationalism, the Internet and the construction of identity. In Palestine Online. I.B.Tauris. https://doi.org/10.50409780755607884/
- Avis, M., Marciniak, D., & Sapignoli, M. (2025). States of Surveillance: Ethnographies of New Technologies in Policing and Justice. Routledge. https://www.routledge.com/Routledge-
- Awwad, G., & Toyama, K. (2024). Digital Repression in Palestine. Conference on Human Factors in Computing Systems - Proceedings, 15. https://doi.org/10.11453613904.3642422/;WGROUP:STRING:ACM
- Bauman, Z. (1989). Modernity and the Holocaust. Cornell University Press.
- Bevilacqua, I. (2022). E-scaping apartheid: Digital ventures of Zionist settler colonialism. Human Geography(United Kingdom), 15(2), 220–228. https://doi.org/10.117719427786211055780/
- Busse, J. (2022). Everyday life in the face of conflict: Sumud as a spatial quotidian practice in Palestine. Journal of International Relations and Development, 25(3), 583. https://doi.org/10.1057/S412681-00255-022-
- Clarno, A. (2018a). Neoliberal Apartheid: Palestine/Israel and South Africa after 1994. In The University of Chicago Press. The University of Chicago Press. https://doi.org/10.11770094306118779814/e
- Clarno, A. (2018b). Neoliberal colonization in the West Bank. Social Problems, 65(3), 323–341. https://doi.org/10.1093/socpro/spw055
- Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
- Fanon, F. (1963). The wretched of the earth. Grove Press.
- Foucault, M. (2008). The Birth of Biopolitics: Lectures at the Collège De France 19781979- (G. Burchell, Tran.). Palgrave Macmillan. https://doi.org/10.22439/fs.v0i7.2640

- Getzoff, J. F. (2020). Start-up nationalism: The rationalities of neoliberal Zionism. Environment and Planning D: Society and Space, 38(5), 811–828. https://doi.org/10.1177026377582091194 9/
- Ghaddar, J. J. (2025). Palestine as provenance: archiving against genocide from Gaza to South Lebanon (Jabal Amil). Archival Science 2025 25:3, 25(3), 20-. https://doi.org/10.1007/S1050209484--025-Y
- Gillespie, T. (2018). Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.
- Giroux, H. A. (2025). Scholasticide: Waging War on Education from Gaza to the West. Https://Doi.Org/10.3366/Hlps.2025.0348, 24(1), 1–16. https://doi.org/10.3366/HLPS.2025.0348
- Hammami, R. (2005). On the Importance of Thugs The Moral Economy of a Checkpoint. Jerusalem Quarterly., (2228–22 ,(23/.
- Johnson, D. (2019). Occupation: Neoliberalism' s Role in Palestinian Apartheid. In Locus: The Seton Hall Journal of Undergraduate Research (Vol. 2).
- Jorisch, Avi. (2018). Thou shalt innovate : how Israeli ingenuity repairs the world. Gefen Publishing House Ltd. https://books.google.com/books/about/Thou_Shalt_Innovate.html?id=k_uEswEACAAJ
- Khoury-Machool, M. (2007). Palestinian Youth and Political Activism: The Emerging Internet Culture and New Modes of Resistance. Policy Futures in Education, 5(1), 17–36. https://doi.org/10.2304/PFIE.2007.5.1.17
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race and Class, 60(4), 3–26. https://doi.org/10.1177030639681882317 2/
- Kwet, M. (2022). Digital Colonialism and Infrastructure-as-Debt. University of Bayreuth African Studies Online, 65–77. https://orcid.org/00005649-3304-0002-.
- Last, D. M. (2007). Economic Peace-Building to Support Israeli-Palestinian Disengagement. In Royal Military College of Canada (Number May).
- Lentin, R. (2020). Palestinian Lives Matter: Racialising Israeli Settler-Colonialism. Journal of Holy Land and Palestine Studies, 19(2), 133–149. https://doi.org/10.3366/HLPS.2020.0238
- Lloyd, D., & Wolfe, P. (2016). Settler colonial logics and the neoliberal regime. Settler Colonial Studies, 6(2), 109–118. https://doi.org/10.10802201473/X.2015.1035361
- Loewenstein, A. (2023). The Palestine Laboratory: How Israel Export the technology of occupation around the world. Verso Books. https://www.researchgate.net/publication/377691958
- Maggor, E. (2020). The Politics of Innovation Policy: Building Israel's "Neo-developmental" State. Politics and Society. https://doi.org/10.11770032329220945527/
- Masalha, N. (2012). Appropriating History: Looting of Palestinian Records, Archives and Library Collections, 19482011-. In The Palestine Nakba Decolonising History, Narrating the Subaltern, Reclaiming Memory (pp. 135–147). Zed Books.
- Mignolo, W. (2009). Epistemic Disobedience, Independent Thought and Decolonial Freedom. Theory, Culture & Society, 26(8), 159–181. https://doi.org/10.11770263276409349275/;WEBSITE:WEBSITE:SAGE;JOURNAL:JOURNAL:TCSA;WGROUP:STRING:PUBLICATION
- Mignolo, W. (2011). Epistemic Disobedience and the Decolonial Option: A Manifesto. TRANSMODERNITY: Journal of Peripheral Cultural Production of the Luso-Hispanic World, 1(2). https://doi.org/10.5070/t412011807
- Mignolo, W., & Walsh, C. (2018). On Decoloniality: Concepts, Analytics, Praxis. Duke University Press. https://books.google.com/books/about/On_Decoloniality.html?hl=it&id=l8hcDwAAQBAJ
- Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond Data Universalism. Television and New Media, 20(4), 319–335. https://doi.org/10.117715274764198/37739;JOURNAL:JOURNAL:TVNA;PAGE:STRING:ARTICLE/CHAPTER
- Musleh, A. H. (2018). Designing in Real-Time: An Introduction to Weapons Design in the Settler-Colonial Present of Palestine. Design and Culture, 10(1), 33–54. https://doi.org/10.108017547075.2018.1430992/
- Noble, S. U. (2018). Algorithms of Oppression How Search Engines Reinforce Racism. NYU Press. https://www.degruyterbrill.com/document/doi/10.18574/nyu/9781479833641.001.0001/html

- Peeters, R., & Schuilenburg, M. (2023). Algorithmic Governance: Technology, Knowledge and Power. In The SAGE Handbook of Digital Society (pp. 439–457). SAGE Publications Ltd. https://doi.org/10.41359781529783193/.n25
- Peled-Elhanan, N. (2012). Palestine in Israeli School Books Ideology and Propaganda in Education. I.B. Tauris.
- Rijke, A., & Van Teeffelen, T. (2014). To Exist Is To Resist: Sumud, Heroism, and the Everyday | Institute for Palestine Studies. Jerusalem Quarterly , (59). https://www.palestine-studies.org/en/node/165375
- Rindova, V., Barry, D., & Ketchen, D. J. (2009). Entrepreneuring as Emancipation. In Academy of Management Review (Vol. 34, Number 3, pp. 477–491). Academy of Management. https://doi.org/10.5465/amr.2009.40632647
- Sabbagh-Khoury, A. (2022). Tracing Settler Colonialism: A Genealogy of a Paradigm in the Sociology of Knowledge Production in Israel. Politics and Society, 50(1), 44–83. https://doi.org/10.11770032329221999906/
- Sabbah-Karkabi, M., & Abu-Rabia-Queder, S. (2025). The politics of silence: Palestinian faculty and the struggle for voice in Israeli academia in times of war*. Ethnic and Racial Studies, 1–19. https://doi.org/10.108001419870.2025.2561759/;JOURNAL:JOURNAL:RERS20 ;REQUESTEDJOURNAL:JOURNAL:RERS20;WGROUP:STRING:PUBLICATION
- Sa'di, A. H. (2021). Israel's settler-colonialism as a global security paradigm. Race and Class, 63(2), 21–37. https://doi.org/10.11770306396821996231/
- Sela, R. (2018). The Genealogy of Colonial Plunder and Erasure–Israel's Control over Palestinian Archives. Social Semiotics, 28(2), 201–229. https://doi.org/10.108010350330.2017.1291140/
- Senor, Dan., & Singer, Saul. (2009). Start-up nation : the story of Israel's economic miracle. In Twelve. Twelve.
- Shalhoub-Kevorkian, N. (2015). Security theology, surveillance and the politics of fear. In Security Theology, Surveillance and the Politics of Fear. Cambridge University Press. https://doi.org/10.1017/CBO9781316159927
- Shalhoub-Kevorkian, N. (2017). Settler colonialism, surveillance, and fear. In Israel and its Palestinian Citizens: Ethnic Privileges in the Jewish State. https://doi.org/10.1017/CBO9781107045316.012
- Shehadeh, H. (2023). Palestine in the Cloud: The Construction of a Digital Floating Homeland. Humanities (Switzerland), 12(4). https://doi.org/10.3390/h12040075
- Shihadeh, M. (2024). The War on Gaza and Israel's Technology Sector. https://arabcenterdc.org/resource/the-war-on-gaza-and-israels-technology-sector/
- Siegel M., S. (2015). Let There Be Water: Israel's Solution for a Water-Starved World. Macmillan.
- Swed, O., & Butler, J. S. (2015). Military capital in the Israeli Hi-tech industry. Armed Forces and Society, 41(1), 123–141. https://doi.org/10.11770095327/X13499562
- Tariq, D. (2024). Gaza's Genocide and Israel's Military-Industrial Complex. https://www.palestine-studies.org/en/node/1655307?utm_source=chatgpt.com
- Tarvainen, A., & Challand, B. (2024). Innovation as erasure: Palestine and the new regional alliances of technology. Transactions of the Institute of British Geographers, 49(2). https://doi.org/10.1111/tran.12663
- Tatour, L. (2019). Citizenship as Domination: Settler Colonialism and the Making of Palestinian Citizenship in Israel. The Arab Studies Journal, 2(27), 839. https://ssrn.com/abstract=3533490
- Tawil-Souri, H. (2012). Digital Occupation: Gaza's High-Tech Enclosure. Journal of Palestine Studies, 41(2), 27–43. https://www.jstor.org/stable/10.1525/jps.2012.xli.2.270%AJSTOR
- Tawil-Souri, H., & Aouragh, M. (2014). INTIFADA 3 . 0 ? CYBER COLONIALISM AND PALESTINIAN RESISTANCE. The Arab Studies Journal, 22(1), 102–133.
- Veracini, L. (2011). Introducing: settler colonial studies. Settler Colonial Studies, 1(1), 1–12. https://doi.org/10.10802201473/X.2011.10648799
- Veracini, L. (2015). The Settler Colonial Present. Springer. https://books.google.it/books?hl=it&lr=&id=1U9OCgAAQBAJ&oi=fnd&pg=PP1&dq=Veracini,+L.+(2015).+The+settler+colonial+present.+Springer.&ots=BHiCY7DQmJ&sig=vLPGe1JJd4qXe_dj_rYKqhZK68s#v=onepage&q=Veracini%2C%20L.%20(2015).%20The%20settler%20colonial%20present.%20Springer.&f=false
- Wildeman, J. (2019). Neoliberalism as Aid for the Settler Colonization of the Occupied Palestinian Territories After Oslo. In Palestine and Rule of Power (pp. 153–174). Springer

International Publishing. https://doi.org/10.10077_1-05949-030-3-978/

- Wind, Maya. (2024). Towers of ivory and steel : how Israeli universities deny Palestinian freedom. 278.
- Wolfe, P. (2006). Settler colonialism and the elimination of the native. Journal of Genocide Research, 8(4), 387–409. https://doi.org/10.10801462352060105624O/
- York, J. C. (2012). PALESTINE ONLINE: TRANSNATIONALISM, THE INTERNET AND THE CONSTRUCTION OF IDENTITY by Miriyam Aouragh. The Arab Studies Journal, 20(1), 214–217. https://www.jstor.org/stable/23265851?seq=1#metadata_info_tab_contents
- Zureik, E. (2001). Constructing Palestine through surveillance practices. British Journal of Middle Eastern Studies, 28(2), 205–227. https://doi.org/10.10801353019012008308 6/
- Zureik, E. (2016a). Israel's colonial project in Palestine: Brutal pursuit. Routledge. https://doi.org/10.43249781315661551//ISRAEL-COLONIAL-PROJECT-PALESTINE-ELIA-ZUREIK/ACCESSIBILITY-INFORMATION
- Zureik, E. (2016b). Strategies of Surveillance: The Israeli Gaza. Jerusalem Quarterly, 66, 21–31.
- Zureik, E. (2020). Middle East Critique Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel. Middle East Critique, 29(2), 219–235. https://doi.org/10.108019436149.2020.1732043/
- Zureik, E., Lyon, D., & Abu-Laban, Y. (2010). Surveillance and control in Israel/ Palestine: Population, territory and power. In Surveillance and Control in Israel/Palestine: Population, Territory and Power. https://doi.org/10.43249780203845967/

أصوات أسيرة:
التجسس الصوتي الخوارزمي في فلسطين

سارة فتح الله

سارة منظِّمة مجتمعية وباحثة نقدية في الذكاء الاصطناعي، ومرشحة ماجستير (MSt) في أخلاقيات الذكاء الاصطناعي والمجتمع بجامعة كامبريدج. تستكشف أبحاث سارة الآثار القسرية/العقابية للتكنولوجيا، وكيف يدعم الذكاء الاصطناعي منطق المراقبة والتجريب والسياسات المميتة ضمن جغرافيات القمع، لا سيما على أسس عنصرية. يمتد عملها بين عدالة الصحة الإنجابية وحقوق العمل وقضايا اللجوء.

يركز بحث سارة في إطار الزمالة على عسكرة الذكاء الاصطناعي ضمن منظومة المراقبة والسيطرة الرقمية الإسرائيلية على الفلسطينيين/ات، لا سيما عبر مراقبة الصوت والالتقاط والطباعة الصوتية البيومترية. وتتحرى ما إذا كانت إسرائيل تبني قاعدة بيانات صوتية قابلة للبحث للفلسطينيين/ات، وتحدد النظم والبُنى التحتية التي تمكّن هذا النظام.

توطئة

بالنسبة للفلسطينيين تحت الاحتلال الإسرائيلي، أصبح الصوت سلاحًا في إحدى أكثر أنظمة التجسس الجماعيّ تطورًا في العالم، مما يحول فعل التحدث إلى فعل أسر. يعكس العنوان «أصوات أسيرة» هذا الفعل: يتم التقاط الأصوات الفلسطينية من خلال أنظمة اعتراض الاتصالات، ليتم تمريرها بأنظمة التحليل الخوارزمي، وتُلتقط في نهاية المطاف ضمن نظام تحّكم وسيطرة يسعى إلى احتواء كل قول كدليل أو مبرر محتمل. يكشف هذا التقرير عن بنية التجسس الصوتيّ الخوارزمية في فلسطين، ويكشف كيف تحوّل فعل الحديث إلى سلاح رقمي بأيدي الاحتلال.

أهمية التجسس الصوتيّ

وُصف نظام التجسس الصوتيّ في إسرائيل بأنه «واحد من أكبر مجموعات بيانات التجسس في العالم وأكثرها تطفلًا على مجموعة سكانية مُعيّنة».[1] ومع ذلك، على الرغم من هذا النطاق، ركز الخطاب العام بشكل أكبر على التجسس بواسطة كاميرات التجسس، وأنظمة التعرف على الوجه، ومراقبة وسائل التواصل الاجتماعي في فلسطين.[2] وفعلًا، احتشد المجتمع المدني بقوة ضد التعرف على الوجه. عام 2023، دعت حملة، إلى جانب أكثر من 170 منظمة من منظمات المجتمع المدني - بما في ذلك منظمة العفو الدولية ومنظمة «هيومن رايتس ووتش» ومؤسسة حرية الإنترنت - إلى فرض حظر عالمي على تقنيات التعرّف على الوجه.[3] وبالمثل، كُتب الكثير عن التجسس على سلوك الفلسطينيين عبر الإنترنت، وتأثيره على حقوقهم الرقمية.[4]

ومع ذلك، لم تجتذب عمومًا طرائق الاتصالات والتجسس القائمة على الصوت سوى القليل من التدقيق البحثي والجماهيري. وحين يكون هناك اهتمام بها، غالبًا ما يميل إلى التأكيد على القيود التقنية لتقنيات الصوت بالذكاء الاصطناعي في السياقات التجارية،[5] عوضًا عن دورها السرطاني في شرطنة وحوكمة شعب بأكمله.

نطاق هذا التقرير

تعترف هذه التقارير بـ»التجسس الصوتي» كشكل أوسع من أشكال التجسس المعنية بالتقاط جميع الأصوات، بشكل يشبه حال الكشف عن الطلقات النارية،[6]

1 يوفال أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين»، 972+ Magazine، 6 آب/ أغسطس 2025، https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/.

2 حملة، تكثيق التجسس في القدس الشرقية منذ أكتوبر 2023 (حملة - المركز العربي لتطوير الإعلام الاجتماعي، 2024)، https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en ؛ صوفيا جودفريند، توسيع نطاق التجسس الرقمي في القدس وتأثيره على حقوق الفلسطينيين (حملة، المركز العربي لتطوير الإعلام الاجتماعي، 2021)، https://7amleh.org/storage/Digital 20Surveillance 20Jerusalem_7.11.pdf ؛ حملة، تقنية التعرّف على الوجه وحقوق الفلسطينيين الرقمية (حملة، المركز العربي لتطوير الإعلام الاجتماعي، 2020)، https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights.

3 منظمة العفو الدولية، منظمة العفو الدولية وأكثر من 170 منظمة تدعو إلى حظر التجسس البيومتري ، 7 حزيران/ يونيو 2021، https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.

4 إياد برغوثي وأليسون كرمل، الشبكات الصامتة: التأثير المروع بين الشباب الفلسطيني في وسائل التواصل الاجتماعي (حملة، المركز العربي لتطوير الإعلام الاجتماعي، 2019)، https://7amleh.org/post/silenced-net-the-chilling Effect-among-palestinian-youth-in-social-media ؛ حملة، الشباب الفلسطينيين والمشاركة السياسية عبر شبكات التواصل الاجتماعي [الشباب الفلسطيني والمشاركة السياسية عبر شبكات التواصل الاجتماعي] (حملة، المركز العربي لتطوير الإعلام الاجتماعي 2019)، https://7amleh.org/wp-content/uploads/10/2019استطلاع-حملة1-.pdf.

5 دانيال لاوفر، «التجسس الصوتيّ: لماذا لا تريد أن يتطفل عليك الذكاء الاصطناعي»، Access Now، 23 أيلول/ سبتمبر 2025، https://www.accessnow.org/ai-snooping/.

6 مؤسسة الحدود الإلكترونية، «كشف الطلقات النارية»، Street Level Surveillance، بدون تاريخ، https://sls.eff.org/technologies/gunshot-detection.

أو قياس التلوث الضوضائي في المناطق الحضرية.[7] كما يصطلح التقرير مفهوم «التجسس الرقمي» كفئة واسعة النطاق تشمل تتبع السلوك عبر الإنترنت، لكنه لا يركز بالضرورة على تتبع الاتصالات المنطوقة.

وبشكل أكثر تحديدًا، يركز هذا التقرير على التجسس الصوتيّ: مراقبة الاتصالات الصوتية واعتراضها وتحليلها، بما في ذلك المكالمات الهاتفية الخلوية، وهي مكالمات تقليدية لشبكة المحمول ذات العلاقة بأرقام الهواتف، والاتصالات الصوتية عبر بروتوكول الإنترنت (VoIP) مثل مكالمات تطبيقات المراسلة والرسائل الصوتية، والتي يتم نقلها عبر الإنترنت ومرتبطة بحسابات التطبيق وليس الأرقام. يغطي التقرير أيضًا البيانات الكبرى (metadata) المتصلة التي توفر سياقًا للأصوات - متى تم نطقها، من قالها، أين، وبواسطة أية أجهزة.

ويركز هذا التقرير أيضًا على الفلسطينيين في الأراضي المحتلة: الضفة الغربية والقدس الشرقية وغزة. لا يغطي نطاق التقرير الحالي اللاجئين الفلسطينيين في الشتات أو في مخيمات اللاجئين والمواطنين الفلسطينيين في إسرائيل، على الرغم من الأدبيات المُعتبرة (في أعمال أحمد ح. سعدي[8]، إيليا زريق،[9] وآخرين[10]) تتناول السياق المذكور.

المنهجية

يتطلب التحقيق بتقنيات التجسس في فلسطين العمل ضد السرية المؤسساتية العميقة، إذ أن الوصول لمعلومات حول عمليات التجسس والعمليات العسكرية الاسرائيلية صعب للغاية. ومع ذلك، يهدف هذا التقرير إلى جمع المعرفة المحدودة المُتوفرة حاليًا للجمهور من مصادر عامة، تقارير إعلامية، وتوثيق المجتمع المدني، باللغتين الإنجليزية والعربية في الغالب.

نظرًا للتعتيم شبه المُطلق المُحيط بالبنية التحتية للتجسس، يتبع نهج التقرير تقليد ما يصفه علماء المعرفة بأنه «التسفية كمنهجية»، أي تجميع القطع بغياب أدلة أمبيرية (تجريبية) كاملة. وبالتالي، فإن التسفية كموقف منهجي هو «استجابة متكيّفة للندرة أو للشحّ»،[11] مما يستدعي الحيلة والاقتدار بمواجهة المعلومات المحجوبة أو المتستر عليها.[12] لا يدعي هذا التقرير أنه يقدم الصورة الكاملة لهيكلية أو مبنى التجسس الصوتيّ في إسرائيل. عوضًا عن ذلك، فإنه يوّفر إعادة بناء حيوية وإن كانت جزئية، حيث تجمع قطع اللغز المُتاحة، والتي، مجتمعة معًا، تكون كافية لإظهار كيف يتم استخراج الكلمات المنطوقة لمجتمع كامل بواسطة أحد أكثر أنظمة التجسس الجماعية نفوذًا في العالم.

7 أليانا ديموبولوس، «هونك هونك! هل يمكن للكاميرات الملتقطة للضجيج أن تقلل من التلوث الصوتي «القاتل المحتمل»؟»، The Guardian (New York)، 4 تشرين الأول/ أكتوبر 2023، https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras.

8 Ahmad H. Sa'di, Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority, Manchester International Relations (Manchester University Press, 2016).

9 Elia T. Zureik, Israel›s Colonial Project in Palestine: Brutal Pursuit, Routledge Studies on the Arab - Israeli Conflict 20 (Routledge, 2016).

10 Usama Halabi, 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel', in Surveillance and Control in Israel/Palestine: Population, Territory, and Power, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), https://doi.org/10.4324/9780203845967.

11 صوفي ماري نيانغ، «دفاعًا عما هو هناك: ملاحظات على التسفية كمنهجية»، Feminist Review 136، رقم 1 (2024): 53، https://doi.org/10.1177/01417789231222606.

12 نيانغ، «دفاعًا عما هو هناك»، 57.

1. خلفية وسياق

1.1. القاعدة التاريخية والتحليلية

لا يمكن فهم جهاز التجسس الصوتيّ الإسرائيلي بمعزل عن سياقه التاريخي والنظام البيئي الأوسع للاحتلال القائم على تقنيات التجسس. تكشف هذه القاعدة التاريخية والتحليلية كيف أن التجسس الصوتيّ لا يعمل كبرنامج تكنولوجي معزول، بل كجزء لا يتجزأ من نظام شامل للتحكم في السكان.

الجذور التاريخية للتجسس الإسرائيلي وتواصله

لم يبدأ التجسس في فلسطين بالعصر الرقمي، ولا حتى بتأسيس إسرائيل. على حد تعبير الباحثة هيلغا طويل - صوري، «ولدت الصهيونية كنظام تجسس».[13] تعود جذور التجسس الإسرائيلي إلى فترة ما قبل عام 1948، عندما قامت الميليشيات الصهيونية بتطوير خدمات التجسس كمساعدين للشرطة والجيش البريطانيين، واخترقت شبكات الاتصالات، وأجرت تجارب على الاعتراض اللاسلكي والتشفير. ما سيحظى لاحقًا بالاسم الرسمي «استخبارات الإشارات» (Signals Intelligence) - التنصت على الأسلاك والتشفير وفك التشفير والمراقبة الإلكترونية - كان مضمنًا بالفعل في المشروع السياسي الذي سبق تشكيل إسرائيل.[14]

بناءً على هذه التعاونات المبكرة مع الانتداب البريطاني، جمعت الجماعات الصهيونية بشكل منهجي معلومات استخباراتية عن الأراضي والسكان والشبكات الاجتماعية. وكما تلاحظ طويل الصوري، فإنهم «تعلموا واستفادوا من أسراب وثائق سلطات الانتداب البريطاني التي تُفصّل وتُحدد جوانب لا تُعد ولا تُحصى للحياة اليومية في فلسطين»، بما في ذلك القوائم الضريبية، ومسوحات الأراضي، والخرائط الهيكلية.[15] أجرت إحدى هذه المجموعات، شاي، «عملية القرية العربية» الضخمة، حيث جمعت بيانات مكثفة عن القرويين والموارد والبنية التحتية والأسلحة وحتى المقاتلين خلال ثورة 1936-1939.[16] وضع هذا التركيز المبكر على أعمال التجسس الأسس والقاعدة لمبنى أجهزة الأمن الإسرائيلي بعد عام 1948. على سبيل المثال، تطوّرات الهيئات القائمة حاليًا مثل الشاباك، جهاز الأمن الداخلي الإسرائيلي الواقع تحت إشراف رئيس الوزراء المُباشرة، من هذه الشبكات لجمع المعلومات قبل قيام الدولة،[17] مما ساهم بإضفاء الطابع الرسمي المؤسساتي على نظام لا يقتصر على أهداف مُحددة فحسب، بل إنه أوسع نطاقًا على صعيد المجتمع ككل.

ترسانة التجسس

ينوّه إلى أهمية استمرار استخدام هذه التقنيات القائمة منذ قبل 1948 بانتظام إلى يومنا هذا. يواصل نظام التجسس الحالي في إسرائيل الاستفادة من التكتيكات

13 محمد ر. مهاوش، «مراقب، متجسس عليه، مُستهدف»، مجلة نيويورك، 3 كانون الأول/ ديسمبر 2025، https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html.

14 Helga Tawil - Sori, 'Israel's Telecommunications Lines and Digital Surveillance Routes', in Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonial after Elia Zureik , ed. Ahmad H. Sa'di and Nur Masalha (I.B. Tauris, 2023), 214–15.

15 Helga Tawil - Sori, 'Surveillance Sublime: The Security State in Jerusalem', Jerusalem Quarterly, no. 68 (December 2016): 58, https://doi.org/10.70190/jq.168.p56.

16 Tawil-Souri, 'Surveillance Sublime', 58.

17 Tawil-Souri, 'Surveillance Sublime', 58.

التقليدية التي تشمل «قوة شرطة، عملاء الاستخبارات، مُخبرين، جواسيس، مُستعربين، مُتعاونين، الاعتقال والسجن، أساليب التعذيب والاستجواب، المُراقبة والتتبع عن بُعد والمراقبة المباشرة، المنشآت والأسس المتباينة، رسم الخرائط، مسوحات الأراضي وسجلاتها وتطويبها، التخطيط الحضري، هندسة العمارة، أبراج المراقبة، السجلات السكانية، الإحصاءات السكانية المجتمعية، بطاقات التعريف والهُويّات الشخصية، وأدوات أحدث قليلًا بتقنيات غير متطوّرة، مثل الاعتراض البريدي، والتنصت على المكالمات الهاتفية، وأجهزة الأشعة السينية».[18] وعلى الرغم من أن إسرائيل اعتمدت بشكل متزايد تقنيات تجسس حديثة - «كالطائرات المُسيّرة، طائرات بدون طيار، الإنسانيات (روبوتات) المُتحكم بها عن بُعد، جمع البيانات البيومترية، والفيروسات الحاسوبية» - إلا أن هذه الأدوات «لا تحل محل الأدوات ذات التقنية غير المتطوّرة، بل إنها تكملها»،[19] مما يدل على أن التجسس في إسرائيل ليس نتاج التقانة الرقمية فحسب، بل هي نظام هجين شامل قائم من زمن بعيد.

توّثق مجموعة كبيرة من الأدبيات والدراسات البحثية الترسانة التجسسية الإسرائيلية. وكما لاحظ الراحل إيليا زريق، فإن التجسس في إسرائيل «يتشكل من استخدام أساليب مثل تسجيل المعلومات الالكترونية من خلال التنصت على الهاتف واعتراض الرسائل الإلكترونية».[20] تُضاف على اعتراض الاتصالات والتجسس عليها، أنظمة التعرف على الوجه وأنظمة بيومترية، البنية التحتية المحسوسة التجسسية المُدمجة في المعابر والحيّزات الحضرية العمرانية، الطائرات المُسيّرة، والإشراف على المحتوى الرقمي في شبكات التواصل الاجتماعية وغيرها من الأنشطة عبر الإنترنت، السيطرة على التنقل ومراجعة الهُويّات، شبكات المُخبرين والمُتعاونين البشريين، وغيرها المزيد.[21]

يجب فهم التجسس الصوتيّ، على الرغم من كونه المِحوَر الوحيد لهذا التقرير، على أنه أحد مركبات نظام بيئي تجسيي مترابط. لا يعمل التجسس الصوتيّ في عزلة ولكنه يُضخَم بفضل أساليب التجسس الأخرى ويُضخِّمها. على سبيل المثال، قد توفر الاتصالات الصوتية التي يتم اعتراضها معلومات تمكن المزيد من الإشراف المُستهدف والدقيق لشبكات التواصل الاجتماعي، في حين أنه يمكن استخدام البيانات من أنظمة التعرّف على الوجه للمقارنة المرجعية مع البصمات الصوتية بهدف إنشاء ملفات تعريف بيومترية أكثر شمولاً. يخلق هذا الترابط نظامًا تعزز فيه أساليب متعددة بعضها البعض لتحقيق السيطرة الكاملة على السكان وقمع واضهاد المقاومة، مما يُدمج التجسس في نسيج الاحتلال نفسه.

دور الخوارزمية في التجسس الصوتيّ

إن المخزون الهائل للصوت المنطوق المخزن الذي تم جمعه من الفلسطينيين لا يقل قيمة عن قدرة إسرائيل على معالجة المعلومات التي يحتوي عليها والبحث فيها. وحيث اعتمدت إسرائيل في التسعينيات على خبراء بشريين للتحقق من

18 Tawil-Souri, 'Surveillance Sublime', 59.

19 Tawil-Souri, 'Surveillance Sublime', 59.

20 Elia Zureik, 'Colonialism, Surveillance, and Population Control', in Surveillance and Control in Israel/Palestine: Population, Territory, and Power, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), 12–13, https://doi.org/10.4324/9780203845967.

21 (IMEU, Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement (Institute for Middle East Understanding, 2021.

هُويات الأفراد المشاركين في محادثة هاتفية والتعرف عليهم،[22] يُشير الحجم الهائل للبيانات الصوتية المجموعة حتى الوقت الراهن، إلى اعتماد إسرائيل المحتمل على تعلّم الآلة والأدوات الخوارزمية، وليس فقط على التعرّف على المتحدثين، بل إلى «اكتشاف المعرفة في قواعد البيانات» على نطاق أوسع.[23]

من المهم ملاحظة أن مثل هذه التقنيات لم تظهر فجأة ولا مؤخرًا فقط. وفقًا للمصادر التي استشهد بها الجارديان، نشرت الوحدة 8200 «منذ ما يقرب من عقد» أنظمة الذكاء الاصطناعي لتحليل الاتصالات التي تم اعتراضها وتخزينها، باستخدام «موديلات تعلّم الآلة على نطاق أصغر» من أجل «فرز المعلومات إلى فئات محددة مسبقًا، وتعلم التعرف على الأنماط واستنباط التوقعات على أساسها».[24]

هناك أيضًا سابقة تثبت قدرة إسرائيل على التحليل الصوتي المُتطوّر. رغم أنهم لم يذكروا الأدوات الدقيقة، أشار باحثو التجسس إيليا زريق ودافيد ليون إلى الصلاحيات الشاملة المعنية بالمراقبة الممنوحة للشاباك والشرطة خلال جائحة كوفيد19-.[25] كما علّق الباحث آفي مارتسيانو على التأطير العسكري الذي اعتمدته السلطات، مقتبسًا قول رئيس الوزراء، الذي أكد خلال مؤتمر صحفي، أنه تم توظيف نفس الأدوات الرقمية المستخدمة ضد الفلسطينيين، في وقت لاحق، ضد الإسرائيليين لتتبع انتشار الفيروس.[26] وحذرت منظمات المجتمع المدني، بما في ذلك حملة، من «مراقبة وتتبع الأشخاص على مدار 24 ساعة في اليوم، 7 أيام في الأسبوع»- بما في ذلك مكالماتهم - المشروعة «بحجة منع انتقال العدوى وانتشارها». [27]

وبالذات أحد أشكال التحليل الذي يمكّن من تحديد هوية الأفراد بحسب صوتهم. في مقال لرويترز يتناول دراسة اختبار صوت أثناء جائحة كوفيد19- أجرتها وزارة الأمن الاسرائيلة، أكد المقال على أنه تم تحليل عيّنات من أصوات المرضى باستخدام خوارزميات التعلم الآلي المُصممة لتحديد العلامات الصوتية الفريدة وتحديد «بصمة صوتية» للتشخيص والمراقبة عن بُعد. تُوّضح الدراسة، أن إسرائيل تملك القدرة التقنية على اجراء تحليل صوتيّ خوارزمي واسع النطاق دون علاقة بالعمليات الاستخباراتية.[28] تساعد هذه السوابق في موضعة البنية التحتية الحالية لمعالجة الصوت والتسجيلات التي يتم اعتراضها. مما يوّفر سياقًا مهمًا لفهم الأدوات التي من المحتمل أن تستخدمها إسرائيل لتحليل بيانات التجسس الصوتيّ على نطاق واسع.

22 دان دي لوس، «الباروكات والبنادق الروبوتية وأجهزة البيجر المتفجرة: لإسرائيل تاريخ طويل في مطاردة أعدائها»، إن بي سي نيوز، 20 أيلول/ سبتمبر 2024، https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888.

23 أسامة فياض وآخرون، «من استخراج البيانات إلى اكتشاف المعرفة في قواعد البيانات»، مجلة الذكاء الاصطناعي ، 15 آذار/ مارس 1996.

24 هاري ديفيز ويوفال أبراهام، «الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين»، الجارديان (القدس)، 6 آذار/ مارس 2025، https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

25 Elia Zureik and David Lyon, 'Coronavirus Surveillance and Minority Groups in Israel/Palestine', The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.

26 Avi Marciano, 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity', Surveillance & Society 19, no. 1 (2021): 85–86, https://doi.org/10.24908/ss.v19i1.14543.

27 حملة، تنتياهو يفرض يتجسس ك «الأخ الأكبر» بحجة الاستجابة الأمنية على جائحة فيروس كورونا، 23 آذار/ مارس 2020، https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response.

28 رويترز، «وزارة الأمن الإسرائيلية تطلق دراسة اختبار صوت كوفيد19-»، رويترز (القدس)، 24 آذار/ مارس 2020، https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/.

الإحتلال الرقمي

أسفر الاحتلال في 1967 عن فترة انتقالية للاقتصاد الإسرائيلي نحو تقنيات الاتصالات المتقدمة بشكل متزايد، في حين حُرم الفلسطينيون من تطوير البنية التحتية لاتصالاتهم السلكية واللاسلكية بشكل مُجدٍ، وعاشوا تحت «نظام عسكري صارم حد من استخدام معظم أشكال الاتصالات من الصحف إلى أجهزة الفاكس».[29] بحلول التسعينيات، واصلت إسرائيل الاستثمار بكثافة في بنيتها التحتية للاتصالات والتجسس، في حين ظلت المناطق الفلسطينية متخلفة من حيث البنية التحتية ويسهل التجسس عليها ومراقبتها.[30] تُشير طويل-الصوري إلى كون الفلسطينيين، فعليًا، «محتجزين إتصالاتيًا».[31]

لم تفلح معاهدات أوسلو عام 1993 بتغيير هذه الظروف للأحسن. في حينه، أقل من 2% من الأسر الفلسطينية كانت تملك خط هاتف أرضي، في حين تملكت قرابة 75% من الأسر الإسرائيلية خطًا أرضيًا. البنية التحتية التي تسلمتها السلطة الفلسطينية كانت متأخرة ومتهالكة، وقد استصعبت شركة الاتصالات الفلسطينية - التي أنشئت عام 1995 لإدارة الاتصالات السلكية واللاسلكية - الاستجابة للطلب على وقع المعيقات والقيود البنيوية التي فرضها الاحتلال، كعدم السيطرة الكاملة على البنية التحتية، واضطرار البنية التحتية المذكورة للتوافق مع الأطر الإسرائيلية المفروضة عليها، واشتراط أن تحصل عمليات اقتناء المعدات «على موافقة إسرائيلية مُسبقة، وحتى في بعض الحالات، الالتزام بشرائها من موردين إسرائيليين مُباشرة».[32] تعيق هذه التبعيات قدرة تكنولوجيا المعلومات والاتصالات الفلسطينية (ICT) على تحقيق الاكتفاء الذاتي. كما أشارت شبكة السياسة الفلسطينية «الشبكة» إلى أن «القيود الشديدة التي تفرضها إسرائيل على القطاع الفلسطيني» قد زادت من الاعتماد على الأنظمة الإسرائيلية وقوضت السيادة الفلسطينية.[33]

يشكل هذا التاريخ العمود الفقري لما تسميه هيلغا طويل الصوري «الاحتلال الرقمي»، الذي يصف السُرادقات المُقيّدة بقيود وشروط وضوابط إسرائيل على «عرض النطاق الترددي؛ موضع، عدد وقوة أجهزة توجيه الإنترنت (راوتر) أو المقاسم (البدالات) الهاتفية؛ نطاق الإشارات الخلوية؛ والمعدات المستخدمة».[34] يتفق الخبراء على أن أي جهة قادرة على «عزل المستخدمين الأفراد أو خدمات اتصال مُعيّنة أو مجتمعات بأكملها» عن النظم البيئية الرقمية تتمتع بقوة كبيرة في أمن المعلومات.[35] بالنسبة للفلسطينيين، هذه الجهة هي إسرائيل. منذ تشرين الأول/ أكتوبر 2023، تم استهداف البنية التحتية للإنترنت والاتصالات السلكية واللاسلكية في غزة - بما في ذلك الأبراج الخلوية، الكوابل، الخوادم، ومكاتب شركتي الاتصالات الفلسطينيتين - عمدًا. تسببت هذه الهجمات، مُجتمعة بقدرة اسرائيل المتواصلة على التحكم بالبنية التحتية الرقمية الفلسطينية، في انقطاع غير مسبوق للإنترنت،

29 طويل سوري، «خطوط الاتصالات السلكية واللاسلكية ومسارات التجسس الرقمية في إسرائيل»، 215–16.

30 طويل سوري، «خطوط الاتصالات السلكية واللاسلكية ومسارات التجسس الرقمية في إسرائيل»، 216.

31 طويل الصوري، «خطوط الاتصالات السلكية واللاسلكية ومسارات التجسس الرقمية في إسرائيل»، 217.

32 طويل الصوري، «خطوط الاتصالات السلكية واللاسلكية ومسارات التجسس الرقمية في إسرائيل»، 217.

33 هيلغا طويل الصوري، «اختراق فلسطين: إحتلال رقمي»، الجزيرة، 9 تشرين الثاني/ نوفمبر 2011، https://www.aljazeera.com/opinions/2011/11/9/hacking-palestine-a-digital-occupation.

34 هيلغا طويل الصوري، «الاحتلال الرقمي: سُرادق غزة عالي التقنية»، مجلة الدراسات الفلسطينية 41، رقم 2 (2012): 28، https://doi.org/10.1525/jps.2012.XLI.2.27.

35 صوفي فلينسبورغ وسيغني سوفوس لاي، «اتبع البيانات! استراتيجية لتتبع قوة البنية التحتية '، وسائل الإعلام والاتصالات 11، رقم. 2 (2023): 323، https://doi.org/10.17645/mac.v11i2.6464.

مما أدى إلى قطع اتصال غزة بنسبة تزيد عن 80%.[36] في مواجهة هذا الدمار واسع النطاق، تتضح معالم ندرة البنية التحتية والتبعية والضعف التي تفرضها إسرائيل والقائمة إلى يومنا هذا.

الاحتلال الرقمي ليس مجرد مصطلح وصفي لسيطرة إسرائيل على البنية التحتية للاتصالات؛ إنه مرتبط جوهريًا بالتجسس الصوتيّ. من الأسهل «تقييد والسيطرة على الأنظمة الأقدم والمحدودة عمدًا والتجسس عليها، سواء عن طريق التنصت أو الكشف عن حركة البيانات ومراقبتها، وحتى القدرة على تعطيلها».[37] من المحتمل أن يتم تعديل المُعدات التي يجب أن تمر عبر الجمارك الاسرائيلية أو أن تُقتنى من موردين اسرائيليين، ومن المحتمل أن يتم تجهيزها لتُتيح التجسس.[38] بما أن الشبكات الفلسطينية معتمدة على البنية التحتية الإسرائيلية ويتم توجيهها في نهاية المطاف عبرها، تحتفظ إسرائيل بإمكانية «تتبع والتقاط وتسجيل حركة الصوت والبيانات والاستخدامات والأنماط برمتها».[39] لا يمكن فصل دور إسرائيل العالمي في مجالات هندسة المستشعرات، التشفير، ومعالجة الإشارات عن مقوّمات الهيمنة الرقمية وبنيتها التحتية التي بنتها بالاحتلال.[40]

العنف اليومي المتطفل للتجسس

تظهر الباحثتان نادرة شلهوب - كيفوركيان وعبير عثمان كيف تحوّل التجسس الإسرائيلي من جمع المعلومات الاستخبارية العلنية إلى شكل مُعيّن من أشكال المراقبة «تستخدمه الدولة الإسرائيلية لاختراق والسيطرة على حيوات الفلسطينيين اليومية وأكثر جوانبها حميمية - الأسرة والعائلة».[41] يخاطب الباحثون الفلسطينيون مدى يومية[42] ودُنيوية[43] تقنيات التجسس الخبيثة، من حيث أنها تسمح «بالتسلل إلى المنازل واختراق الاتصالات».[44] يُعتبر التجسس الصوتيّ، الذي يلتقط المحادثات بين أفراد الأسرة الواحدة والأقارب والمحبوبين داخل منازلهم ومجتمعاتهم، واحدة من أوضح التعديات على هذه المساحات العلائقية.

تحمل الطبيعة الانتهاكية للتجسس الصوتيّ أصداء حميمة داخل حياة الفلسطينيين الخاصة ومجتمعاتهم. وصف الجنود الإسرائيليون المُسرحون من الخدمة، حجم ونطاق التنصّت على المحادثات الخاصة أوالحميمية، مُشيرين إلى ما يمكن وصفه بأنه «لا قيود على ما يستطيع الجنود فعله بالمحادثات التي اعترضوها».[45] وأضاف أن «الجنود يقومون بحفظ المحادثات وإرسالها إلى أصدقائهم»، في إشارة إلى تتفيه والتقليل من شأن الخصوصية في صفوف أصحاب القدرة على الوصول لبيانات التجسس الصوتيّ. يتماشى هذا مع مشروع التجسس الصوتيّ ككل: في نظام مميت

36 زها حسن و ح. أ. هيلير، قمع المعارضة: تقلص الحيز المدني والقمع العابر للأوطان وفلسطين - إسرائيل (45–144، Oneworld Academic، 2024).

37 طويل الصوري، «خطوط الاتصالات ومسارات التجسس الرقمي الإسرائيلية»، 219.

38 طويل الصوري، «خطوط الاتصالات ومسارات التجسس الرقمي الإسرائيلية»، 219.

39 طويل الصوري، «خطوط الاتصالات ومسارات التجسس الرقمي الإسرائيلية»، 219.

40 الطويل الصوري، «خطوط الاتصالات ومسارات التجسس الرقمي في إسرائيل»، 220.

41 نادرة شلهوب - كيفوركيان وعبير عثمان، «السرية كعنف استعماري: حالة القدس الشرقية المحتلة»، في إنهاء استعمار دراسة فلسطين: وجهات نظر السكان الأصلانيين والاستعمار الاستيطاني بعد إيليا زريق، محرر. أحمد ح. سعدي ونور مصالحة Secrecy as Colonial Violence, 188, (I.B. Tauris, 2023).

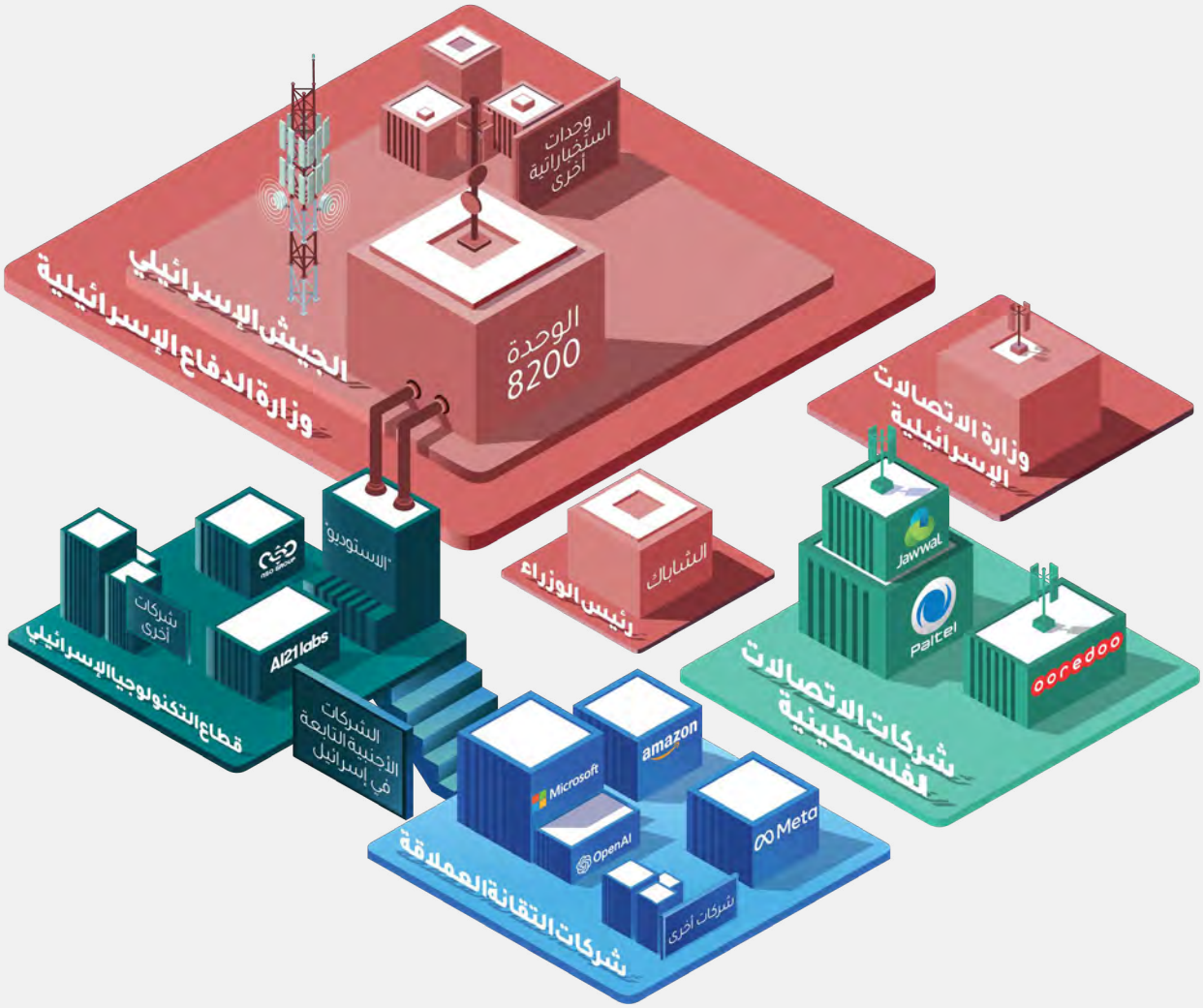
42 Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear, 1st edn (Cambridge University Press, 2015), 27, https://doi.org/10.1017/CBO9781316159927.

43 زريق، المشروع الإستعماري الاسرائيلي في فلسطين، 109.

44 Rajaie Batniji, 'Searching for Dignity', The Lancet 380, no. 9840 (2012): 466, https://doi.org/10.1016/S0140-6736(12)61280-X.

45 لُبنى مصاروة، «تستطيع إسرائيل مراقبة جميع المكالمات الهاتفية في الضفة الغربية وغزة، بحسب مصدر استخباراتي»، ميدل إيست آي (القدس)، 15 تشرين الثاني/نوفمبر 2021، https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.

للتحكم الكلي في عدد السكان، لا تكون الخصوصية مستحيلة بشكل فعال فحسب، بل لا تتعارض مع الحاجة إلى معرفة الفلسطينيين الرازحين تحت الاحتلال.



1.2. الجهات المتورطة في التجسس الصوتيّ

بناءً على الأسس التاريخية والتحليلية أعلاه، من الأهمية بمكان تحديد الجهات الفاعلة التي تشكل بشكل جماعي نظام التجسس الصوتيّ في فلسطين، كما هو مُوّضح بشكل مختصر في الرسم البياني أدناه. وتشمل هذه الجهات، وكالات حكومية، شركات إسرائيلية خاصة، شركات تقانة متعددة الجنسيات، ومزوّدي خدمات الاتصالات الفلسطينيين العاملين في بيئة تحت السيطرة الاسرائيلية.

الحكومة والجيش الإسرائيلي

في صميم بنية التجسس الصوتيّ توجد الوحدة 8200، الوحدة الاستخباراتية في الجيش الإسرائيلي التي تتبع الاشارات وأكبر وحدة في الجيش الإسرائيلي.[46] الوحدة 8200 هي الجهة الفاعلة الرئيسية التي تراقب اتصالات الفلسطينيين الصوتية،

46 الخصوصية الدولية، صناعة التجسس العالمية (2016)، 23، https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

وتعترض مكالماتهم وتسجلها، وتخزن ملفاتهم الصوتية، وتعالج بياناتهم وتحللها، بمساعدة شركات خاصة تقنيًا وبأدواتها.

ويكمل عملها الشاباك، الذي يتمتع بالسلطة القانونية للوصول إلى بيانات الاتصالات السلكية واللاسلكية من شركات الاتصالات الإسرائيلية،[47] وهو أحد المتلقين الرئيسيين للبيانات الصوتية، مما يجعله جهة فاعلة مركزية أخرى في منظومة التجسس الصوتيّ.

ومن الجهات الفاعلة الهامة الأخرى هي وزارة الاتصالات الإسرائيلية، التي تسيطر بشكل مباشر على البنية التحتية الفلسطينية لتكنولوجيا المعلومات والاتصالات. فهي تُدير الطيف الخلوي بالكامل، كما أن «وزارة الاتصالات الإسرائيلية هي التي تحدد مقدار عرض النطاق الترددي» المسموح به.[48] علاوة على ذلك، يُطلب من الفلسطينيين الساعين للحصول على معدات تكنولوجيا المعلومات والاتصالات «الحصول على موافقة من وزارة الاتصالات الإسرائيلية لكل شحنة يطلبونها».[49] ويتوجب على الشبكة الفلسطينية أن تنخرط في نظام الشبكة الإسرائيلية، مما يضمن «توافقها مع المعايير المعتمدة والمطبقة في إسرائيل من قبل وزارة الاتصالات».[50]

قطاع التكنولوجيا الخاص في إسرائيل

قطاع التجسس الخاص في إسرائيل واسع للغاية لدرجة أمست البلاد الأكثر كثافة في العالم بعدد شركات التجسس للفرد الواحد،[51] مما يشكل أكبر سوق لاستخلاص البيانات واسع النطاق.[52] تتعزز قدرات التجسس العسكري الاسرائيلية بفضل صناعة التقانة الخاصة هذه، على وقع «التنسيق القوي بين وزارة الأمن و [...] الشركات المدنية».[53] أحد مخرجات هذا التعاون هو «الاستوديو»، المركز القائم داخل الوحدة 8200 التجسسية. وفقًا لتقارير إخبارية، تم تطوير العديد من أدوات التجسس القائمة على الذكاء الاصطناعي هناك من خلال ربط الجنود في الخدمة الفعلية مع جنود الاحتياط العاملين في شركات التكنولوجيا، الذين ساهموا في «المعرفة والوصول إلى التقنيات الرئيسية التي لم تكن متاحة في الجيش».[54]

عدّد تقرير صادر عام 2016 من منظمة الخصوصية الدولية، والذي يقيّم حالة التجسس على مستوى العالم، والذي شمل دراسة حالة افرادية خاصة بإسرائيل، على الأقل جهة فاعلة واحدة في التجسس الصوتيّ، و 15 جهة فاعلة في المتابعة والمراقبة الهاتفية، إلى جانب أكثر من اثني عشر جهة أخرى فاعلة في التقنيات

47 المرصد الأورومتوسطي لحقوق الإنسان، يجب على شركات الاتصالات الإسرائيلية الالتزام بمبادئ الأمم المتحدة، ووقف التعاون الكامل مع الأجهزة الأمنية، 13 تشرين الثاني/ نوفمبر 2022، https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles, - stop-fully- cooperating-with-security-agencies.

48 طويل الصوري، «الاحتلال الرقمي»، 33–35.

49 وسيم ف. عبد الله وسام بحور، تكنولوجيا المعلومات والاتصالات: المُحرّك المُقيّد لتنمية فلسطين (الشبكة، 2015)، 7، https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.

50 Xavier Stephane Decoster et al., The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development, no. 104263 (World Bank Group, 2016), 61, http://documents.worldbank.org/curated/en/993031473856114803.

51 الخصوصية الدولية، صناعة التجسس العالمية، 23.

52 سارة فتح الله ونيك ميتشل، «الأصول المحتلة: النيوليبرالية الإسرائيلية واستخراج البيانات من حيوات الفلسطينيين»، مجلة مفاصل، كانون الثاني/ يناير 2026، https://disjunctionsmag.com/articles/occupied-assets/.

53 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

54 تايمز أوف إسرائيل، «إسرائيل تستخدم الذكاء الاصطناعي لتحديد قادة حماس، والعثور على رهائن في أنفاق غزة — تقرير»، تايمز أوف إسرائيل، 26 نيسان/ أبريل 2025، https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.

الأخرى ذات صلة محتملة بمنظومة التجسس الصوتيّ، كالمراقبة عبر الإنترنت والاختراق (تثبيت برامج التجسس في أجهزة الاتصال).[55] تشمل الشركات الإسرائيلية المعروفة التي تسوّق برامج التجسس الصوتي والقياسات الحيوية وتقنيات التحليلات المواتية بشكل نشط، كل من Corsound AI و Cognyte و MultiKol و Nemesysco و NiCE و PerSay و Verint، بالإضافة إلى شركات برامج التجسس مثل Candiru و Cellebrite و Cytrox و Paragon.

شركات التكنولوجيا الأجنبية

تلعب الشركات متعددة الجنسيات - مثل «مايكروسوفت» و«أمازون» - أدوارًا أساسية بتوفير خدمات التخزين السحابي والذكاء الاصطناعي (AI) من خلال عقود حكومية كبيرة مثل مشروع «نيمبوس».[56] تمتلك شركات التكنولوجيا العملاقة أيضًا شركات تابعة ومراكز بحث وتطوير وبنى تحتية للخوادم في إسرائيل،[57] والتي ثبت ضروريتها في البنية التقنية والعملياتية لمشروع التجسس الصوتي الإسرائيلي.

شركات الإتصالات الفلسطينية

أخيرًا، تعمل شركات الاتصالات الفلسطينية - «جوال» و «أوريدو فلسطين» - في إطار نظام السيطرة الإسرائيلي على الطيف الترددي والبنية التحتية للمعدات وواردتها. وكما أسلفنا، فإن هذه التبعية تُمكّن السلطات الإسرائيلية من مراقبة الاتصالات الصوتية الفلسطينية القائمة على الشبكة الخلوية، تصنيفها وفرزها، واعتراضها. يُشار إلى كون هذه التبعية في انتهاك مُباشر لمعاهدات أوسلو».[58] الداعية للامتناع «عن أي عمل يتعارض مع أنظمة الاتصالات والبث والبنى التحتية الخاصة بالجانب الآخر».[59]

1.3. تتبع البيانات (التجسس الصوتيّ)

بعد أن قمنا برسم خارطة الجهات الفاعلة المعنية، تستدعي الخطوة التالية لفهم منظومة التجسس الصوتيّ الاسرائيلية تتبع حركة البيانات الصوتية، من الالتقاط إلى الاستخدام. يعتمد هذا النهج على إطار عمل حددته الباحثتان صوفي فلينسبورغ وسيغن سوفوس لاي، وبحسبه، مثلما تتبع التحقيقات في هياكل السلطة وأنظمة الأعمال في كثير من الأحيان الأموال، على دراسات الاقتصادات السياسية الرقمية «أن تتبع البيانات».[60] من شأن هذا الأمر أن يكشف كيف تتم ممارسة التعاون والعلاقات الارتكازية المتبادلة، وكيف أنها تُصان وتُضخّم بفضل البنى التحتية للبيانات، عبر شبكات وصول، أنظمة رقمية أساسية، تطبيقات، وخدمات البيانات.[61]

يُتيح لنا النظر إلى حالة فلسطين من هذا المنظور تتبع كيف تنتقل الاتصالات

55 الخصوصية الدولية، صناعة التجسس العالمية.

56 الجزيرة، «ما هو مشروع نيمبوس، ولماذا يحتج عمال جوجل على صفقة اسرائيلية؟»، الجزيرة، 23 نيسان/ أبريل 2024، https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal.

57 اينفستيجيت، «Amazon.Com Inc.»، لجنة أصدقاء الخدمة الأمريكيين، 7 آب/ أغسطس 2024، https://investigate.info/company/amazon؛ اينفستيجيت، «Microsoft corp.»، لجنة أصدقاء الخدمة الأمريكيين، 29 كانون الثاني/ يناير 2005، https://investigate.info/company/microsoft.

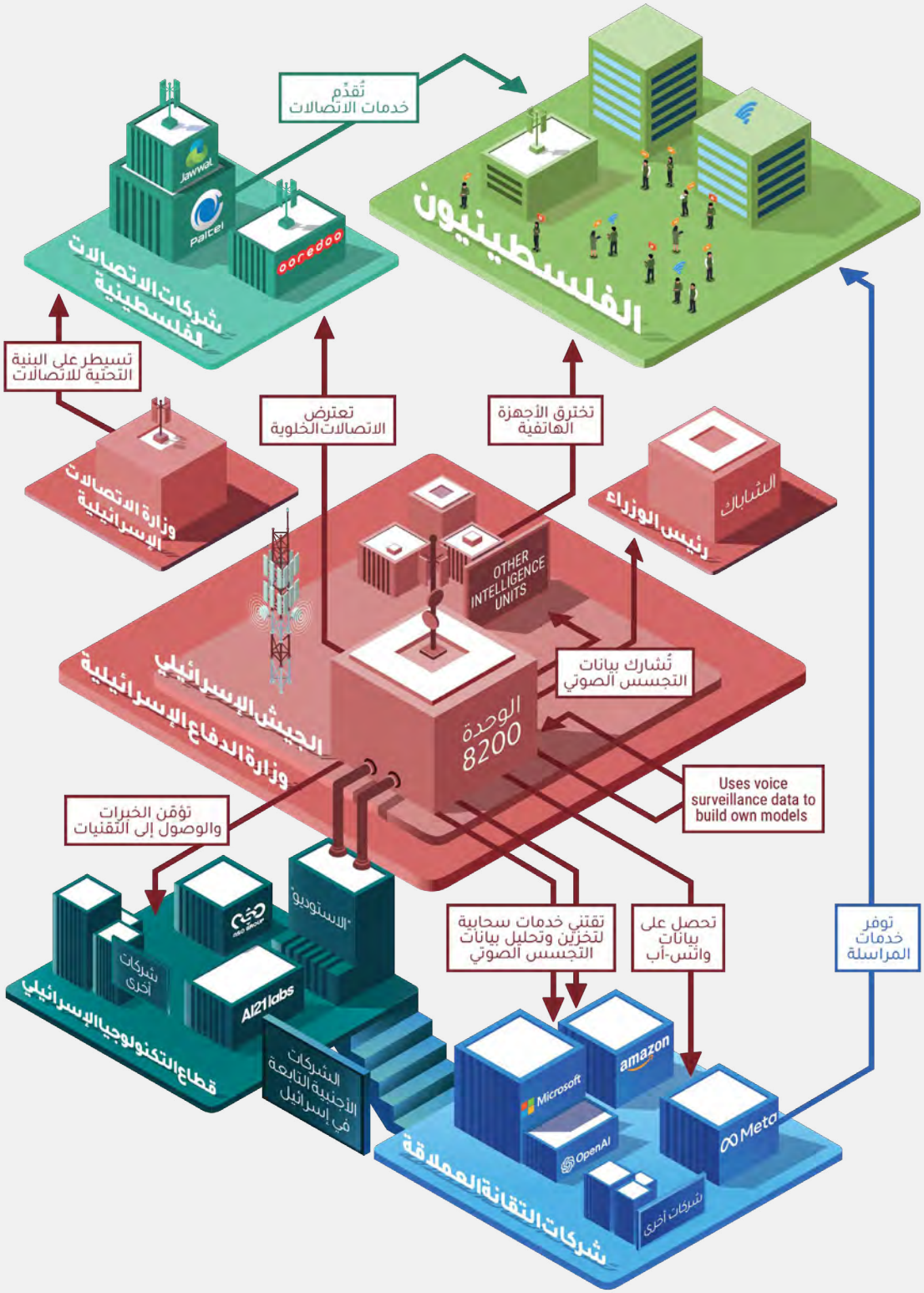
58 داني أوبراين وجيليان سي. يورك، «سفينة بطيئة نحو البيانات السريعة: لماذا لا تزال فلسطين تنتظر 3G؟»، مؤسسة الطليعة الالكترونية، 11 تشرين الثاني/ نوفمبر 2015، https://www.eff.org/deeplinks/2015/11/palestine-3g.

59 معاهدات أوسلو، الملحق الثالث، حول الشؤون المدنية، الاتفاق الإسرائيلي الفلسطيني المؤقت بشأن الضفة الغربية وقطاع غزة (أوسلو 2) (1995)، 35–36، https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.

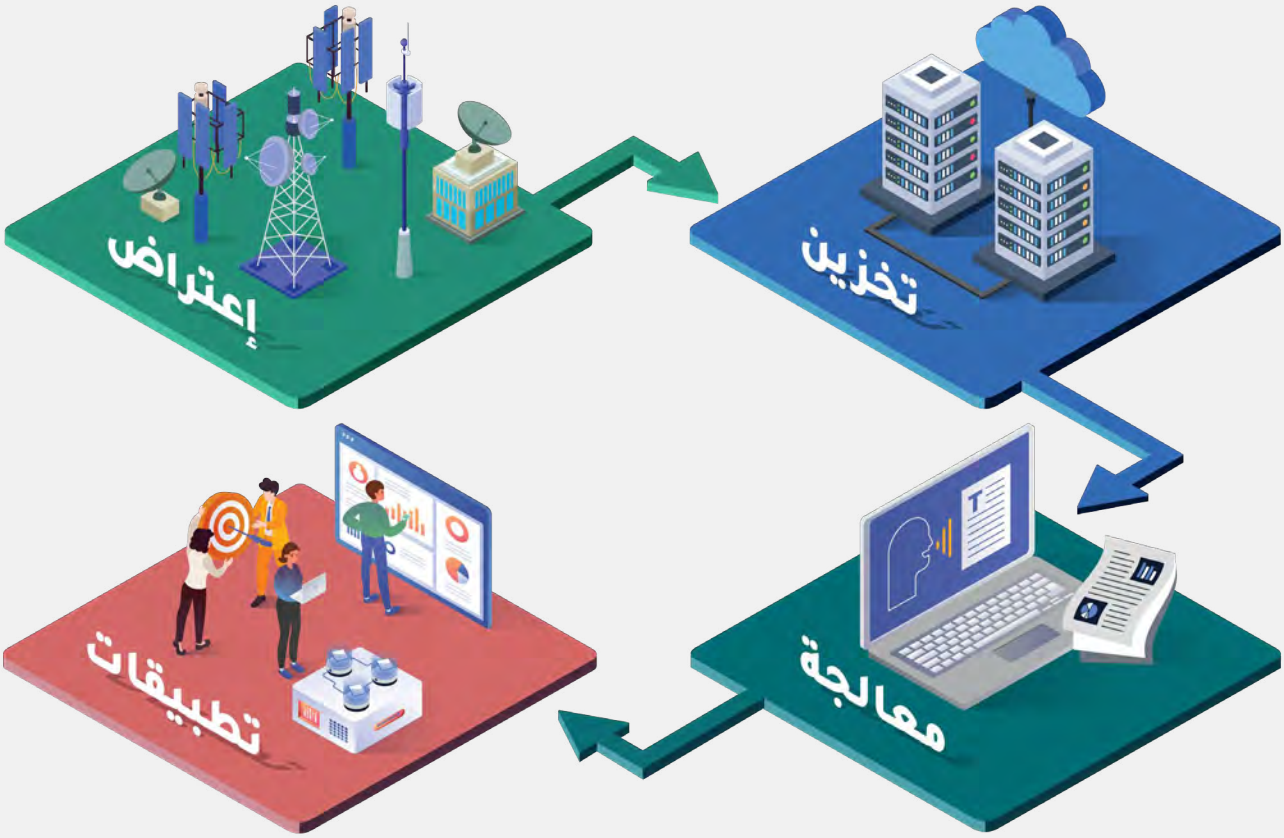
60 فلينسبورغ ولاي، «اتبع البيانات! إستراتيجية لتتبع قوى البنية التحتية «، 319.

61 فلينسبورغ ولاي، «اتبع البيانات! استراتيجية لتتبع قوى البنية التحتية «، 319–20.

الصوتية من محادثات عادية إلى أيدي شبكة من الجهات المتخصصة بالتجسس، حيث تُصوّر العلاقات فيما بينها في الرسم أدناه، والتي سنعاينها بعدسة محققة أكثر تفصيلًا في الأقسام التالية.



بتتبع بيانات التجسس الصوتيّ، يُبنى هذا التقرير على أربع خطوات: إعتراض الاتصالات والتقاط البيانات الصوتية (القسم 2)، تخزين بيانات التجسس الصوتيّ والاحتفاظ بها (القسم 3)، معالجة وتحليل بيانات التجسس الصوتيّ (القسم 4)، وتطبيقات بيانات التجسس الصوتيّ (القسم 5). في حين تُعرض بشكل متسلسل، فإن هذه الخطوات هي جزء من عملية متواصلة وتكرارية، نموذجية للبنى التحتية الخاصة بالبيانات.



2. إعتراض البيانات الصوتية والتقاطها

2.1. الفلسطينيون الخاضعون للتجسس الصوتيّ

ما بدأ كمراقبة تستهدف أفراد مُحددين قد توسع إلى نظام تجسس صوتيّ على مستوى مجتمع كامل. يصف هذا القسم النطاق الحالي للتجسّس الصوتيّ في فلسطين، والمجموعات التي تستفردها للتدقيق المُشدد، ونطاقها الجغرافي الآخذ بالاتساع.

تجسّس جماعيّ على كل فلسطينيّ

يبلغ نطاق التجسس الصوتيّ الإسرائيلي على الفلسطينيين نطاقًا واسعًا، ويستهدف الجميع. وقد أشارت الصحافية لُبنى مصاروة في تقريرها عبر مجلة «ميدل إيست

آي» عام 2021 أن «إسرائيل يمكنها الاستماع إلى أي محادثة في الضفة الغربية وقطاع غزة»،[62] وتوضح أنه «في أي وقت من الأوقات، يستمع مئات الجنود إلى المحادثات الجارية ببث حي ومباشر».[63] في حين أن هذا المقال شكّل تجديدًا للقرّاء الناطقين باللغة الإنجليزية (والدوليين)، نوّه وجدي الجعفري عام 2014، عبر مقالة في وكالة «معا» الإخبارية إلى أن إسرائيل تراقب جميع وسائل الاتصال في فلسطين، بما في ذلك من خلال الهواتف المحمولة والخطوط الأرضية، بموجب إفادات لمسؤولين فلسطينيين.[64] على سبيل المثال، تحدث سليمان الزهيري، نائب وزير الاتصالات وتكنولوجيا المعلومات، عن جهاز التجسس الإلكتروني للوحدة 8200 المستخدم لاعتراض المكالمات الهاتفية، من بين أمور أخرى.[65]

تُتاح القدرة بالتجسس على كل فلسطيني وفلسطينية بدلًا من أهداف مُختارة، بفضل الوصول المتزايد للتخزين السحابي واستخدام الحوسبة السحابية. في إطار تحقيق نُشر عام 2025 حول «مشروع إسرائيل الطموح لتخزين مجموعة كبيرة من المكالمات الهاتفية الفلسطينية على خوادم مايكروسوفت في أوروبا»، وصفت صحيفة الغارديان نظام التجسس هذا بال»عشوائي»، كونه يُتيح «لضباط المخابرات بإعادة تشغيل محتوى مكالمات الفلسطينيين الخلوية، والتقاط محادثات مجموعة أكبر بكثير من المدنيين العاديين».[66] بينما، قبل هذه الشراكات مع عمالقة الحوسبة السحابية، كان الجيش الإسرائيلي قادرًا فقط على تخزين «مكالمات بضع عشرات الآلاف من الفلسطينيين» الذين تم مسبقًا تحديدهم كأهداف للتجسس، على أن يتم تخزين المكالمات فقط على خوادم داخلية.[67] مع إتاحة وصوله إلى التخزين السحابي، لم يعد الجيش الإسرائيلي بحاجة لتقييد نفسه بتحديد أهداف التجسس.[68]

جماعات مُعيّنة مُستهدفة ذات أهمية خاصة

على ضوء ذلك، ذكر التقرير ذاته في «ميدل إيست آي» عام 2021 أنه في صفوف المجتمع الفلسطيني الواسع، توجد فئتين تحملان أهمية خاصة لأجهزة الجيش والأمن الداخلي الإسرائيلية. وهي: (1) الفلسطينيون الناشطون سياسيًا ، و (2) الأفراد الذين تعرضهم ظروفهم الشخصية للابتزاز. ترتكز هذه الجماعات ذات الأهمية الخاصة على سوابق طويلة الأمد. قبل أكثر من عقد، إعترف جنود سابقون في الوحدة 8200 بمراقبة مدنيين فلسطينيين من أجل جمع معلومات شخصية حساسة، لاحتمال الضغط عليهم، كما «اعترفوا بتتبع النشطاء السياسيين».[69]

عندما يتعلق الأمر بالمجموعة الأولى، أكد محامي حقوقي أن الشاباك «منزعج بشكل خاص من النشطاء السلميين، لأن هؤلاء الناس يمكنهم قيادة حركة شعبية وتوليد

62 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

63 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

64 وجدي الجعفري، «مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة»، وكالة معًا الاخبارية، 20 كانون الأول/ ديسمبر 2014، https://www.maannews.net/news/748592.html.

65 الجعفري، «مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة».

66 هاري ديفيز ويوفال أبراهام، «مليون مكالمة في الساعة »: إسرائيل تعتمد على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين»، الجارديان، 6 آب/ أغسطس 2025، https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

67 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

68 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

69 يوفال أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين»، مجلة 972 +، 6 آذار/ مارس 2025، https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.

احتجاجات واسعة النطاق».[70] ويرى أن «أكثر ما يقلقهم هو منظمات المجتمع المدني، لأنه بوسع نشاطها أن يؤول إلى إنهاء الاحتلال، خصوصًا، أنها تحظى بتعاطف المجتمع الدولي».[71] يُعتبر التجسس على الناشطين السياسيين الفلسطينيين أساسيًا في مساعي إسرائيل لقمع المقاومة.

أما المجموعة الثانية، التي أطلق عليها أحد الجنود السابقين في الجيش الإسرائيلي لقب «نقاط الضغط»، فهي تشمل الأشخاص الذين يُجبرهم الشاباك على «التعاون أو الكشف عن شؤون شخصية تخص آخرين» بسبب ميولهم الجنسية، أمراض، مديونية، أو ظروف أخرى تعنيهم أو أحد أفراد العائلة المقربين، في ممارسة للسيطرة والتهديد.[72]

التركيز الجغرافي والتوسع

من الناحية الجغرافية، ركز التجسس الصوتيّ في البداية على السكان الفلسطينيين في الضفة الغربية. في السنوات الأخيرة، توّسعت المنظومة لتشمل غزة أيضًا.[73] بعد أكتوبر 2023، أوضح ضابط مخابرات لمجلة «972+» أن «الحماس الداخلي لتخزين بيانات التجسس الجماعي من غزة على النظام القائم على السحابة زاد»، مشيرًا إلى أن الهدف هو التوجه «نحو السيطرة طويلة الأجل هناك، كما هو الحال في الضفة الغربية».[74] ومع ذلك، أعربت مصادر لـ«الجارديان» عن مخاوفها بشأن كيفية تأثر مشروع التجسس الصوتي بتدمير البنية التحتية للاتصالات السلكية واللاسلكية في غزة،[75] مما «قلل من حجم المكالمات الهاتفية في المنطقة».[76]

يثير التوسع من التجسس الصوتيّ المُستَهدف للأفراد إلى التجسس الصوتيّ على مستوى المجتمع، وتوّسعه الجغرافي من الضفة الغربية ليشمل غزة أيضًا، والزيادة الكبيرة في قدرة الجمع التي توفرها البنية التحتية السحابية، أسئلة حاسمة حول أشكال البيانات التي يتم التقاطها.

2.2. البيانات المُلتقطة

التسجيلات الصوتية للمحادثات

تشير التقارير المتاحة إلى أن النظام يقوم بأرشفة تسجيلات مُكالمات الفلسطينيين يوميًا، في شكل ملفات صوتية - وليس فقط بيانات نصية،[77] في أرشفة لـ«ملايين مُكالمات الفلسطينيين الخلوية يوميًا في غزة والضفة الغربية».[78] تشكل هذه التسجيلات الصوتية المُعترضة لُب مخزون التجسس الصوتي.

70 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

71 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

72 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

73 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

74 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

75 محمد الشرفاء، تأثير حصار غزة وتدمير البنية التحتية للاتصالات على الاقتصاد الرقمي في خضم الإبادة الجماعية (حملة – المركز العربي لتطوير الإعلام الاجتماعي، 2025)، https://7amleh.org/post/gaza-digital-economy-collapse-en ؛ حملة، البنية التحتية للاتصالات في غزة: تقييم الأضرار والأثر الإنساني (حملة – المركز العربي لتطوير الإعلام الاجتماعي، 2024)، https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en.

76 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

77 يوفال أبراهام، «طلبية من أمازون »: كيف يخزن عملاقة التكنولوجيا بيانات جماعية لحرب إسرائيل»، مجلة 972+، 4 آب/ أغسطس 2024، https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/ ؛ ديفيز وأبراهام، «مليون مكالمة في الساعة »: إسرائيل تعتمد على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين» ؛ أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

78 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

البيانات الوصفية (ميتاداتا) المواتية

بالإضافة إلى الملفات الصوتية، تجمع المنظومة البيانات الوصفية المواتية المرتبطة بكل مكالمة. بينما تكشف الملفات الصوتية عما يُقال، تقدم البيانات الوصفية معلومات حول المشاركين في المكالمات الهاتفية، الوقت، كما جهات الاتصال والموقع.[79] من الراجح أن تشمل بيانات التجسس الصوتي الوصفية المستخرجة مع المكالمات الهاتفية، وقت ومدة المكالمة، طوابع التاريخ والوقت، مصدر ووجهة المكالمة، الجهات المشاركة في المكالمة، مالك الجهاز أو بطاقة SIM المرتبطة بالمكالمة، والمزيد. وقد أشير في تقرير لصحيفة «الجارديان»: «تتضمن المكالمات الهاتفية التي تم اعتراضها والمرتبطة بملف تعريف شخص ما [...] الوقت الذي اتصل فيه الشخص وأسماء وأرقام الأشخاص المشاركين بالمُكالمة».[80]

على الرغم من توفير البيانات الوصفية لمعلومات سياقية تخص المُحادثة الصوتية بالأساس، إلا أنه يمكن استنباط وتخمين الكثير منها حول محتوى المحادثة أيضًا. ويبيّن المحامي أسامة حلبي هذه المسألة بواسطة مثال، مشيرًا إلى أنه، إذا كشفت البيانات الوصفية مثلًا، «أن صحفيًا اتصل بمصدر معين، فقد يكون من الممكن التأكد بدرجة كبيرة من محتوى المكالمة من محض كونها قد تمت».[81]

البيانات المحتملة المتعلقة بواتس-أب

إفترضت تقارير ظهرت عام 2024 أن من المحتمل أن تتعدى البيانات المُلتقطة بواسطة نظام التجسس الصوتيّ المُكالمات التقليدية بالاتصالات السلكية واللاسلكية، لتشمل المعلومات المرتبطة بمُكالمات واتصالات واتس-أب.[82] أثار المراقبون احتمال قيام إسرائيل بجمع البيانات ذات علاقة بالواتس-أب رغم عدم الوضوح إزاء ما إذا كان هذا يشمل فقط البيانات الوصفية أو أيضًا محتوى الاتصالات مثل الملاحظات الصوتية وتسجيلات المكالمات داخل التطبيق. إذا ما صحّت دقة هذه التقارير، فهي تُشير إلى نطاق أوسع بكثير للبيانات المُلتقطة، يشمل نشاط شبكة الاتصالات والمراسلات الصوتية عبر التطبيقات.

2.3. طرق الاعتراض

يعتمد التجسس الصوتيّ الإسرائيلي للفلسطينيين على طرق اعتراض متعددة القائمة على الوصول المباشر إلى البنية التحتية للاتصالات السلكية واللاسلكية واختراق الأجهزة الفردية الخاصة. هناك آليتان موثقتان بشكل جيّد - وهما التنصت على الهواتف ومراقبة شبكات تكنولوجيا المعلومات والاتصالات في الأراضي الفلسطينية المحتلة. وآلية ثالثة، لا تزال غير مُؤكدة، تُعنى بالاعتراض المحتمل للبيانات من تطبيقات المراسلة المشفرة أمثال واتس-أب.

79 روبن جيمس، «التجسس الصوتيّ والبيانات الضخمة»، Sounding Out!، 20 تشرين الأول/ أكتوبر 2014، https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/.

80 مايكل بيسيكر وآخرون، «في وقت تستخدم إسرائيل فيه نماذج الذكاء الاصطناعي الأمريكية الصنع في الحرب، تنشأ مخاوف بشأن الدور الذي تلعبه التكنولوجيا في مسألة الحياة والموت»، أسوشيتد برس نيوز (تل أبيب)، 18 شباط/ فبراير 2025، https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.

81 حلبي، «التحليل القانوني ونقد بعض طرق التجسس التي تستخدمها إسرائيل»، 215.

82 صدى سوشيال، تدعو صدى سوشيال إلى إجراء تحقيق فوري في قيام ميتا بتسريب بيانات مُستخدمي واتس-أب للجيش الإسرائيلي ، 18 أيار/ مايو 2024، https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdmy-oatsab-l-algysh-alsrayly ؛ ربيعة علي، «هل يعرض واتس-أب الفلسطينيين لخطر القتل في غزة؟»، الأناضول، 30 نيسان/ أبريل 2024، https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563 ؛ بول بيغار، ميتا والخُزامى (اللافندر)، 16 نيسان/ أبريل 2024، https://blog.paulbiggar.com/meta-and-lavender/.

إختراق الأجهزة من خلال العيوب البرمجية المُضمّنة وبرامج التجسس

تتضمن إحدى طرق الاعتراض المؤكدة لبيانات التجسس الصوتيّ الاختراق الفعلي المحسوس للهواتف الخلوية الداخلة إلى غزة. قال عضو سابق في استخبارات الإشارات لـ»ميدل إيست آي» عام 2021 إن «كل هاتف خليوي أو هاتف مستورد إلى غزة عبر معبر كرم أبو سالم [...] يحتوي على عيب (Bug) إسرائيليّ مُبرمج».[83] يشير استخدام مصطلح «مُضمّن/يحتوي» إلى آلية قائمة على الأجهزة بدلًا من برامج التجسس (Spyware) القائمة على البرامج، مما يشير إلى تضمين وإدخال مكوّن إلكترونيّ يجعل من الهاتف إلى جهاز استماع. يتماشى هذا التفسير مع تصريحات سابقة لوزير الاتصالات الأسبق مشهور أبو دقة، الذي أشار عام 2014 إلى أن إسرائيل منعت دخول الأجهزة - وخاصة بعض المعدات الصينية - التي وجدت صعوبة في اختراقها أو التنصت عليها،[84] مما يؤكد بدرجة أكبر استخدام الاعتراض القائم على الأجهزة.

يمكن أيضًا اختراق الهواتف من خلال برامج التجسس، والتي يمكنها تنشيط ميكروفون الجهاز سرًا والوصول إلى مجموعة واسعة من البيانات. أحد أكثر الأمثلة شهرة هو برنامج بيجاسوس التابع لمجموعة NSO. تعتبر «هيومن رايتس ووتش» أن برنامج بيجاسوس قادر على تحويل الهاتف «إلى أداة تجسس محمولة من خلال الوصول إلى كاميرا الهاتف والميكروفون والرسائل النصية».[85] تم التأكد بشكل موثوق من حالة واحدة لاستخدام «بيجاسوس» على الفلسطينيين بموجب بحث تقني أجرته عام 2021 مؤسسة «فرونت لاين ديفندرز».[86] وفي وقت لاحق وبشكل مستقل راجع «مختبر المواطن» بجامعة تورنتو و»مختبر الأمن» التابع لمنظمة العفو الدولية البحث، اللذان أجريا تحليلًا وخلصا إلى «أنه تم اختراق أجهزة ستة مدافعين فلسطينيين عن حقوق الإنسان باستخدام برنامج التجسس بيجاسوس من NSO في عامي 2020 و 2021».[87]

التحكم في البنية التحتية للاتصالات

تنبع آلية اعتراض مؤكدة ثانية من سيطرة إسرائيل البنيوية على شبكات الاتصالات الفلسطينية، التي قمنا بتفصيلها في الفصل الأول. كما أوضح أحد المصادر لـ»ميدل إيست آي»، «أي شخص يستخدم إحدى شبكتي الهاتف الخليوي الوحيدتين الفاعلتين في الأراضي الفلسطينية المحتلة [جوال ووطنية - أوريدو فلسطين] خاضع للمراقبة».[88]

لاحظت مؤسسة «إلكترونيك فرونتير» عام 2015 أن إسرائيل قد فرضت قيودًا على شركتي الشبكات الخليوية الفلسطينيتين، لتجبرهم على استخدام تكنولوجيا الهاتف الخليوي من الإصدارات الأقدم «الأكثر عرضة للاستغلال»، وحظرت الوصول

83 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

84 الجعفري، «مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة».

85 هيومن رايتس ووتش، برامج التجسس المستخدمة لاختراق المدافعين عن حقوق الفلسطينيين، 8 تشرين الثاني/ نوفمبر 2021، https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders.

86 فرونت لاين ديفندرز، الأراضي الفلسطينية المُحتلة/إسرائيل: تم اختراق ستة مدافعين فلسطينيين عن حقوق الإنسان باستخدام برامج التجسس Pegasus من مجموعة NSO (فرونت لاين ديفندرز، 2021)، https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware.

87 منظمة العفو الدولية، اختراق أجهزة مدافعين فلسطينيين عن حقوق الإنسان باستخدام برنامج التجسس بيجاسوس من مجموعة NSO، 8 تشرين الثاني/ نوفمبر 2021، https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.

88 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

إلى الأنظمة الأحدث «الأكثر أمانًا من التجسس غير المباشر»،[89] مما يمكّن إسرائيل من «التجسس والتنصت [...] على حركة البيانات عبر شبكات الشركات الإسرائيلية» دون اكتشافها.[90] بغياب هذه الدرجة من السيطرة، كانت اسرائيل ستضطر للجوء إلى طرق تجسس تتطلب دورًا فاعلًا أكثر، كاستخدام تقنيات تجسس أمثال IMSI (الهوية الدولية لمشتركي الهواتف الخليوية). إلا أنه، بعكس التجسس غير المُباشر، التجسس الفعلي النشط أكثر قابلية للاكتشاف.

ولوج مُحتمل لاتصالات واتس-أب

سؤال آخر وإن كان لا يزال دون جواب، يتناول إذا كانت إسرائيل قادرة على الوصول والولوج لاتصالات عبر تطبيق واتس-أب، والتي من المفترض أن تكون محتوياتها مشفرة. تؤكد تقارير من لمجلة 972+ و»سيحا مكوميت» نقلًا عن ستة ضباط استخبارات إسرائيليين، استخدام محادثات بين الفلسطينيين على واتس-أب لتغذية نظام توليد الأهداف الإسرائيلي، «لافندر». أثارت التقارير أسئلة من مراقبين، بما في ذلك مؤسس Tech for Palestine بول بيجار، الذي تساءل «من أين حصلوا على هذه البيانات؟ هل تُشاركها واتس-أب معهم؟»[91] من جانبه، نفى متحدث باسم واتس-أب قيام الشركة بتوفير مدخل خلفي أو «معلومات بالجملة» لأي حكومة، في تلميح لاسرائيل أيضًا.[92] ومع ذلك، حذّر بيان صحافي لمؤسسة المجتمع المدني «صدى سوشيال» عام 2024، شركة «ميتا» مما اعتبرته المؤسسة «تسريبًا للبيانات الفلسطينية» بما يشمل اتصالاتهم عبر واتس-أب.[93] وقد طرح البعض احتمال أن تكون إسرائيل حصلت على بيانات واتس-أب من خلال طرق أخرى غير التسريب أو من مدخل خلفي. وقد ذكر الصحافي مارك أوين جونز احتمال أن تكون اسرائيل قادرة على الوصول لبيانات واتس-أب بطرق أخرى، كالمخبرين أو القرصنة أو برامج التجسس على سبيل المثال.[94] هذه ليست فرضية مجنونة أو غير معقولة، حيث أنه في تشرين الأول/ أكتوبر 2025، قدّم قاضي أمريكيّ أمرًا احترازيًا لشركة «ميتا» بمنع برامج NSO التجسسية من استهداف مستخدمي واتس-أب، والصحافيين والمحامين ونشطاء حقوق الإنسان منهم على وجه التحديد،[95] وهو أمر قضائي سعت NSO ناشطة لإلغائه.[96] علاوة على ذلك، رجّح خبراء آخرون كالناشطة إسراء الشافعي أن إسرائيل قد تتمكن من الوصول إلى «البيانات الوصفية وحدها»، التي تكشف بذاتها «عن الأعضاء بالمجموعة، شبكات جهات الاتصال، وأنماط الاتصال، ولكن ليس محتوى المحادثة.[97]

89 أوبراين ويورك، «قارب بطيء للبيانات السريعة: لماذا لا تزال فلسطين تنتظر الجيل الثالث 3G»

90 أوبراين ويورك، «قارب بطيء للبيانات السريعة: لماذا لا تزال فلسطين تنتظر الجيل الثالث 3G»

91 بيجار، ميتا ولافندر.

92 علي، «هل يُعرّض واتس-أب الفلسطينيين لخطر القتل في غزة؟»

93 صدى سوشيال، صدى سوشيال تدعو إلى إجراء تحقيق فوري في تسريب «ميتا» لبيانات مستخدمي واتس-أب للجيش الاسرائيلي.

94 مارك أوين [@marcowenjones] جونز، «السؤال حول استخدام لافندر لمجموعات واتس-أب لتوليد أهدافها، ودور ميتا المحتمل في هذا الشأن مهم»، 17 نيسان/ أبريل 2024، https://x.com/marcowenjones/status/1780501998728540589?ref_src=twsrc%5Etfw.

95 الجزيرة، «المحكمة الأمريكية تمنع شركة برامج التجسس الإسرائيلية من استهداف مستخدمي واتس-أب»، الجزيرة، 18 تشرين الأول/ أكتوبر 2025، https://www.aljazeera.com/news/2025/10/18/us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users.

96 سوزان سمالي، «تسعى NSO إلى إلغاء ملف واتس-أب، واصفة إياها بالكارثية لمُنتجي برامج التجسس»، ذي ريكورد، 20 تشرين الثاني/ نوفمبر 2025، https://therecord.media/nso-seeks-to-overturn-whatsapp-case.

97 جوليا كونلي، «تقرير يشير إلى أن إسرائيل تستخدم بيانات واتس-أب في عمليات القتل المستهدفة للفلسطينيين»، Truthout، 19 أيار/ مايو 2024، https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/.

3. تخزين البيانات الصوتية والاحتفاظ بها

يعتمد اعتراض إسرائيل الجماعي للاتصالات الصوتية الفلسطينية على مبنى هيكلي متعدد الطبقات للتخزين، مدعومًا من مزودي الخدمات السحابية الكبار وممارسات احتفاظ مرنة. تُحتفظ كميات هائلة من التسجيلات الصوتية والبيانات الوصفية المرتبطة بها عبر منصات وخدمات Microsoft Azure و Amazon Web Services (AWS)، على ما يبدو داخل إسرائيل وفي مراكز البيانات في الخارج، مما يعكس حجم التجسس واعتماد الجيش على البنية التحتية السحابية التجارية.

3.1. مقدمي خدمات التخزين السحابي

لقد جعل حجم ونطاق التجسس الصوتيّ الإسرائيلية للفلسطينيين الاعتماد على مقدمي الخدمات السحابية التجارية أمرًا ضروريًا. يتعدى حجم البيانات - الذي يضم مليارات الملفات الصوتية والبيانات الوصفية المرتبطة بها - الكم المعقول القابل للتخزين على الخوادم التابعة للجيش. وبالتالي، الكثير من البيانات الصوتية المُعترضة تُستضاف في السحابة، على Microsoft Azure وAWS بالمقام الأول، في حين يُواصل الاحتفاظ ببعض البيانات على خوادم الجيش الاسرائيلي بحسب تقارير، إلا أن التفاصيل حول التخزين المحلي تبقى محدودة.

Microsoft Azure

كشفت تقارير نشرتها «ذي جارديان»، مجلة 972+، و«سيحا ميكوميت» في 2025، بحسب وثائق مسرّبة من مايكروسوفت ومقابلات مع نحو 12 مصدرًا من مايكروسوفت والجيش الاسرائيلي، أن الوحدة 8200 نقلت تسجيلات المكالمات الفلسطينية إلى «منطقة مخصصة ومنفصلة داخل منصة Microsoft Azure السحابية».[98] ويشمل ذلك البيانات الصوتية من سكان غزة.[99] إعداد هذه البيئة السحابية هو نتاج التعاون الوثيق بين مهندسي مايكروسوفت والوحدة 8200، بدءًا من عام 2022، بهدف إنشاء نظام «مصمم بعناية لتلبية احتياجات الوحدة».[100] بعض موظفي مايكروسوفت المعنيين كانوا بأنفسهم أعضاء سابقين في الوحدة 8200، عامل ساهم بحسب مصادر «بتسهيل التعاون أكثر».[101] يشكل هذا التعاون جزءًا من شراكة أوسع وأكثر امتيازًا بين مايكروسوفت وإسرائيل، حيث يُنظر إلى عملاق التكنولوجيا كشركة ذات «بصمة مُميّزة في جميع البنى التحتية العسكرية الرئيسية في إسرائيل».[102]

Amazon Web Services

بالإضافة إلى مايكروسوفت، توفر أمازون أيضًا التخزين السحابي لبيانات التجسس الصوتيّ الإسرائيلية. أفاد تحقيق آخر لمجلة 972+ و«سيحا ميكوميت» أن AWS تستضيف البيانات المُجمعة عبر التجسس الجماعي على سكان غزة، بما في ذلك مليارات الملفات الصوتية.[103] وليس واضحًا إذا ما كان هذا التخزين يتم في

98 ديفيز وأبراهام، «مليون مكالمة في الساعة «: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
99 ديفيز وأبراهام، «مليون مكالمة في الساعة «: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
100 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».
101 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».
102 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».
103 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

إطار مشروع «نيمبوس» - عقد مُبرم بين جوجل وأمازون والحكومة والجيش الإسرائيليين، بقيمة 1,3 مليار دولار للخدمات السحابية والذكاء الاصطناعي، علمًا أن معظم طلبات الاقتناء من أمازون وجوجل تتم بموجب العقد المذكور. على غرار مايكروسوفت، تُعتبر أمازون أيضًا كمن تعمل بشراكة وثيقة مع إسرائيل، حيث تزود «مديرية الاستخبارات العسكرية الإسرائيلية بكتلة خوادم تستخدم لتخزين كميات كبيرة من المعلومات الاستخباراتية».[104]

يبدو أن التقارير المتاحة للجمهور حول دور أمازون تشير إلى أن تخزينها لبيانات التجسس الصوتيّ يركز بشكل أكبر على سكان غزة، حيث لا تشير التقارير المذكورة صراحة إلى الضفة الغربية أو القدس الشرقية المحتلة. وفقًا لمصادر عدة، يُتيح نظام سحابة AWS العام للجيش الإسرائيلي «تخزين لا حد له» للاحتفاظ بالمعلومات الاستخبارية عن تقريبًا «الجميع» في غزة.[105] رغم استخدام هذا النظام منذ نهاية عام 2022، إلا أن دوره العملياتي قد توّسع بشكل عظيم بعد أكتوبر 2023.[106]

الاعتماد على البنية التحتية السحابية لشركات التقانة العملاقة

تقر المصادر العسكرية الإسرائيلية بأن حجم بنية التجسس الصوتيّ الخاصة بها يستلزم الاعتماد على مزودي الخدمات السحابية في شركات التقانة العملاقة، لأنها «كبيرة جدًا بحيث لا يمكن تخزينها على الخوادم العسكرية وحدها».[107] على حد تعبير الضابط المسؤول عن مُديرية التحول الرقمي في إسرائيل في مقابلة عام 2020، «لا يستطيع الجيش منافسة الموارد التي يستثمرها عمالقة السحابة وبقية مقدمي الخدمات السحابية في بناء السحابة الخاصة بهم، لذلك لا جدوى من محاولة منافستهم».[108] لهذا السبب، خلصت قيادة الوحدة 8200 إلى أن «سعة التخزين غير المحدودة تقريبًا» لـAzure ضرورية لتخزين اتصالات مجتمع بأكمله، بل أنها كانت تطمح لتوسيع هذه العملية بشكل مُعتبر لتتضاعف «عشرة أضعاف في السنوات القليلة المُقبلة».[109]

3.2. موقع مراكز البيانات والخوادم

سلّطت أحدث التقارير الضوء على التوزيع الجغرافي للبنية التحتية المستخدمة لتخزين بيانات التجسس الصوتيّ الإسرائيلية للفلسطينيين. تم الاحتفاظ بجزء كبير من هذه البيانات - التي تصل إلى آلاف التيرابايت - خارج إسرائيل، في المقام الأول في مراكز بيانات Microsoft Azure الموجودة في أوروبا.

مراكز البيانات الأوروبية

وفقًا لتحقيق مشترك لدى جارديان، مجلة 972+، و«سيحا ميكوميت»، «تشير ملفات مُسربة من مايكروسوفت إلى أن نسبة كبيرة من البيانات الحساسة التابعة للوحدة قد تكون موجودة الآن في مراكز بيانات الشركة في هولندا وأيرلندا».[110] بحلول تموز/ يوليو 2025، ورد أن منشأة خاصة بـ Microsoft Azure - مجمع لمراكز

104 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».
105 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».
106 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».
107 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».
108 جوش ميتنيك، «هكذا يتبنى الجيش الإسرائيلي التحوّل الرقميّ»، CIO، 8 شباط/ فبراير 2020.
109 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
110 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

بيانات بمساحة نحو 14 ألف متر مربع قرب ميدينمير شمال هولندا - استضافت 11,500 تيرابايت من البيانات العسكرية الإسرائيلية، قيل أنها نحو 200 مليون ساعة من الملفات الصوتية.[111] في تقرير آخر أعده نفس فريق التحقيق، أشار إلى أن الحديث عن «نحو 8,000 تيرابايت من البيانات»،[112] مما يعكس بعض التباين في التقديرات المتاحة للجمهور ولكن لا يزال يسلط الضوء على الحجم الهائل للبيانات الصوتية المخزنة.

كما شكلت إيرلندا مركزًا أوروبيًا آخر، وليس ذلك بالمفاجئ، كونها موطن مقر مايكروسوفت الأوروبي.[113] رغم التحفظ عن نشر الأرقام الدقيقة، تشير التقارير إلى أن «نسبة أصغر» من مُجمل البيانات - مقارنة بالحجم المُخزن في هولندا - مُخزنة في خوادم Microsoft Azure هناك.[114]

نقل البيانات بتسارع بعد الكشف للجمهور

عُقب نشر التحقيق المشترك الكاشف لهذه التدابير بالتفصيل، يبدو أن الوحدة 8200 تحركت بسرعة لاستخراج أرشيفات التجسس الصوتيّ التابعة لها من سطوة ولاية قضائية واحدة على الأقل للاتحاد الأوروبي. وفقًا لمصادر مطلعة على عملية النقل، تم نقل البيانات «في غضون أيام»، مطلع آب/ أغسطس 2025. كما رجّح مسؤولون بأجهزة استخبارات أنه تم نقل البيانات إلى خوادم Amazon Web Services (AWS)، وهو ما لم يؤكده الجيش الإسرائيلي ولا أمازون.[115]

التخزين داخل إسرائيل

بعكس التفاصيل الوافدة عن البنية التحتية الأوروبية، لا يزال موقع وحجم الخوادم داخل إسرائيل مبهمًا أكثر. قبل الانتقال للخدمات السحابية، كانت الوحدة 8200 تخزّن مكالمات من اعتبرتهم مسبقًا «مشتبهين» للتجسس عليهم، على خوادمها الداخلية الخاصة.[116] حتى قبل قرار نقل التخزين من خوادم مايكروسوفت في هولندا، يُزعم أن الوحدة 8200 خططت أن تنقل نحو 70% من بيانات التجسس الصوتي إلى Azure،[117] مما يُشير إلى أن بعض مخزون البيانات الصوتية سيظل على الأقل في إطار البنية التحتية للتخزين التابعة للوحدة.

ومن غير الواضح ما إذا كانت هذه البيانات المتبقية موجودة على خوادم الجيش الخاصة أو في المرافق التي تديرها مايكروسوفت وأمازون داخل إسرائيل. قامت الشركتان بتوسيع بنيتهما التحتية لمراكز البيانات التابعة لهما في السنوات القليلة الماضية، حيث دشنت مايكروسوفت مجمعًا لمركز بيانات في إسرائيل عام 2020[118]

111 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

112 هاري ديفيز ويوفال أبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين»، ذي جارديان، 25 أيلول/ سبتمبر 2025، https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

113 ليزا أوكارول، «مطالبة السلطات الأيرلندية بالتحقيق مع مايكروسوفت حول معالجة مزعومة غير قانونية للبيانات من قبل الجيش الإسرائيلي»، ذي جارديان، 4 أيلول/ ديسمبر 2025، https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf.

114 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

115 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».

116 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

117 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

118 مايكروسوفت، مايكروسوفت تدشن مجمع مركز البيانات السحابية الجديدة في إسرائيل، 22 كانون الثاني/ يناير 2020، https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/.

وأمازون عام 2023.[119] ومع ذلك، لا توضح المصادر العامة مكان تخزين بيانات التجسس الصوتيّ داخل إسرائيل.

3.3. فترات الاحتفاظ بالبيانات

لا يزال احتفاظ إسرائيل بالبيانات الصوتية الفلسطينية التي تم اعتراضها مرنًا من الناحية العملية. وفقًا لمصادر استخباراتية في التحقيقات الأخيرة إزاء التخزين في Microsoft Azure، يتم عادة الاحتفاظ بتسجيلات المُكالمات - يشمل لأرقام اسرائيلية ودولية - «في السحابة لمدة شهر تقريبًا».[120] ومع ذلك، أكدت هذه المصادر أن تمديد فترة الاحتفاظ عند الطلب ممكن، مما يمكّن الوحدة 8200 من الاحتفاظ بالتسجيلات لفترات أطول بكثير «عند الحاجة».[121] تم تصميم بيئة التخزين والمعالجة القائمة على Azure للسماح للضباط «بإعادة تشغيل وتحليل محتوى المكالمات الخلوية لمجتمع بأكمله».[122] مما يعني أن ضباط الاستخبارات يمكنهم سحب محادثات الأفراد الذين أصبحوا فيما بعد «محط اهتمام» بأثر رجعي، مما يجعل سياسة الاحتفاظ لشهر إلى أرشيف انتقائي طويل الأجل عمليًا.[123] لا توجد معلومات متاحة للجمهور حول فترات الاحتفاظ ببيانات التجسس الصوتيّ المخزنة في Amazon AWS.

4. مُعالجة البيانات الصوتية وتحليلها

يُوّضح هذا القسم بالتفصيل الأدوات الخوارزمية التي قد تُوظف في معالجة بيانات التجسس الصوتيّ وتحليلها، وتحديدًا للتعرّف على المتحدثين، نسخ الصوت المسجل، ترجمته، وتحليل محتويات الكلام.

4.1. التعرف على المُتحدّث

بعبارات مُبسطة، من المرجح أن تستند قدرة إسرائيل على التعرّف على المشاركين في المكالمات المُعترضة إلى طريقتين واسعتين لتحديد هُويّة المتحدثين: الاستدلال القائم على البيانات الوصفية والبصمة الصوتية البيومترية. وليس من الضرورة أن يكون الأمر حصرًا على أحد النهجين.

الاستدلال القائم على البيانات الوصفية

تعتمد الطريقة الأولى على المعلومات المُستخرجة من البيانات الوصفية للاتصالات، ولا سيما بطاقات SIM المستخدمة لإجراء مكالمة أو تلقيها. من خلال ربط معرّف بطاقة SIM بسجلات المشتركين، تستطيع السلطات أن تقلّص احتمالات مجموعة المتحدثين المرتبطين بمالك البطاقة وأسرته أو شبكته الاجتماعية. حتى حينما يختلف المتحدث عن المالك المُسجل، قد يتمكن المحللين من استنباط من يستخدم الجهاز في أي وقت كان عن طريق الأنماط في شبكاتهم وقوائم الاتصال

119 دان سوينهو، AWS تدشن مجمع سحابي إسرائيلي في تل أبيب، 2 آب/ أغسطس 2023.
120 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
121 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
122 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».
123 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

الخاصة بهم. وقد جاء في تقرير لوكالة الأنباء أسوشييتد برس AP، أن المكالمات المُعترضة «المُرتبطة ببروفيل شخص ما تتضمن أيضًا الوقت الذي اتصل فيه الشخص وأسماء وأرقام الأشخاص المشاركين بالمُكالمة».[124]

البصمة الصوتية البيومترية

الطريقة الثانية، البصمة الصوتية، هي تقنية بيومترية تستمد توقيعًا صوتيًا فريدًا من الخواص الفسيولوجية للفرد (على سبيل المثال، شكل مسرب النطق، الزردمة - أي فُتحة الحُنجرة بين الحبلين الصوتيين وممر الهواء بينهما، التجويف الأنفي) وأنماط الكلام السلوكية (على سبيل المثال، اللهجة، النغمة، أسلوب التحدث). يشير الباحثون في جامعة بوليتكنك فلسطين إلى أن البصمة الصوتية تحمل مزايا فريدة مقارنة بالطرائق البيومترية الأخرى، موضحين أن «البصمة الصوتية لا تتطلب أجهزة خاصة مثل مستشعر بصمات الأصابع أو معدات مسح قزحية العين، بل تتطلب فقط ميكروفونًا رخيصًا من السهل الحصول عليه».[125] ولا تحتاج اسرائيل أن تشتري أو تحصل على الميكروفونات حتى، بالذات تلك المُركّبة بالهواتف الخلوية.

تؤكد العديد من المقالات التعليقية مؤخرًا - وبالأساس مقالات الرأي - أن إسرائيل توّظف استخدام التعرّف على البصمة الصوتية على نطاق واسع. يرى مُحلل السياسة الخارجية ماركو موساد بمقالاته المنشورة في «المجلة» أن الجيش الإسرائيلي أنشأ «مكتبة صوتية»،[126] ويقوم بمتابعة مكالمات للمسلحين «من خلال هواتفهم، والتنصّت على مكالماتهم مع الأقارب وأفراد الأسرة، ثم قام بتسجيل كل صوت، وخلق بصماتهم الصوتية الفريدة في قواعد البيانات»،[127] مما يُتيح التعرف السريع على الشخصيات أثناء عمليات التنصت، كما يُزعم. ويورد باحث السياسة السيبرانية خالد وليد محمود ادعاءات مماثلة في «ذي بينينسولا» واصفًا استخدام «مكتبات صوتية ضخمة» لمطابقة الصوت الذي تم اعتراضه حديثًا مع الملفات الشخصية المُخزنة، ويُشير إلى أن دقة النظام تزداد مع التقاط المزيد من المكالمات.[128] كما ادعى اللواء المتقاعد فايز الدويري، في «الجزيرة»، أن إسرائيل جمعت أصوات ما يقرب من 37000 فرد في بداية حملتها العسكرية الأخيرة في غزة.[129]

رغم أن هذه التقارير تقدم سردية متسّقة، إلا أنها لا تقدم مصادر يمكن التحقق منها. ومع ذلك، يتبين من تقارير سابقة أنه تمت مناقشة هذه القدرات في وسائل الإعلام الفلسطينية لأكثر من عقد من الزمان. عام 2013، أكد الباحث في الشؤون الأمنية سمير محمود قديح لصحيفة «فلسطين اليوم» أن إسرائيل توّظف البصمات الصوتية بعد التنصت على المكالمات الهاتفية وتتبع سجلات مكالمات

124 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

125 محمد عطية صلاح وآخرون، «نظام مصادقة بصمة الصوت» (جامعة بوليتكنك فلسطين، 2021)، https://scholar.ppu.edu/bitstream/handle/123456789/7547/Voiceprint-Authentication-System.pdf.

126 ماركو موساد، «هل عمالقة التكنولوجيا العالمية يسهلون حرب إسرائيل على غزة ؟»، المجلة، 31 أيار/ مايو 2024، https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza.

127 ماركو موساد، «تقنية استنباط البصمة الصوتية: ضربة تجارية ذات فائدة عسكرية»، المجلة، 7 شباط/ فبراير 2024، https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility.

128 خالد وليد محمود، «البصمة الصوتية: من أداة للتحقق من الهوية إلى تقنية التتبع»، ذي بينينسولا، 19 كانون الثاني/ يناير 2025، https://thepeninsulaqatar.com/opinion/19/01/2025/voiceprint-from-a-verification-tool-to-a-tracking-technology.

129 الدويري: الاحتلال يستخدم بصمة الصوت والعين لتعقّب مقاتلي المقاومة بغزة، الجزيرة، 15 نيسان/ أبريل 2025، https://www.aljazeera.net/news/الدويري-الاحتلال-يستخدم-بصمة-الصوت.

الأهداف المستهدفين وجهات اتصالهم كاملة.[130] المونيتور (2014)[131] وردد موقع «رأي اليوم» (2016) هذه الادعاءات، مُضيفًا أن ميكروفونات الجهاز يمكن أن تلتقط الصوت حتى عند تعطيل الهواتف (إطفاءها)،[132] وهو ما تستطيع برامج التجسس المتقدمة فعله من خلال محاكاة حالة إيقاف تشغيل الهاتف لخداع المستخدم بينما يظل الجهاز قيد التشغيل وتحت سيطرة خبيثة.[133]

أسئلة مفتوحة حول مزوّدي التكنولوجيا

من ناحية، يرجح أن تقوم وحدات الاستخبارات الاسرائيلية بالتعرّف على هُويّات المُتحدثين عبر البيانات الوصفية بواسطة البيانات المُعترضة من خلال مراقبة الشبكات الخلوية، ربما بالتعاون مع وزارة الاتصالات الإسرائيلية. هذه الفرضية تصبّ في طور التخمين المدروس والحدس المنطقي.

من ناحية أخرى، على الرغم من الإشارات المتكررة إلى التعرّف بواسطة البصمة الصوتية، فإن المعلومات المتاحة للجمهور لا توضح ما إذا كانت هذه الأنظمة قد قام الجيش الإسرائيلي بتطويرها داخليًا، أو أنه اقتناها من موردين محليين من القطاع الخاص، أو من مزوّدين دوليين. يشمل القطاع الخاص في إسرائيل عددًا كبيرًا من الشركات ذات قدرات التحليل الصوتي المتقدمة، ومن المعروف أن الوحدة 8200 تقوم بتطوير تقنياتها الخاصة. وبالتالي، يظل مصدر أدوات تحديد هُويّة المتحدث سؤالًا يتطلب الجواب.

4.2. تنضيد وتدوين الكلام وترجمته

يتطلب نظام التجسس الصوتيّ في إسرائيل تنضيد وتدوين الكلام وترجمته على نطاق واسع. يشار إلى العملية الأولى، تنضيد وتدوين الكلام، تقنيًا باسم التعرف التلقائي على الكلام (ASR - automatic speech recognition) أو تحويل الكلام إلى نص (STT - speech-to-text) مع اختلافات بسيطة بينهما لا علاقة لها بالتقرير الحالي وغالبًا ما يتم توظيفها بشكل متقطع. العملية الثانية، ترجمة الكلام، تختلف عن تنضيد وتدوين الكلام. إلا أن مُعظم المصادر المتاحة تأتي على ذكرهما مجتمعتين، ولأغراض هذا التقرير، سيتم التعامل معها كمجموعة مشتركة من القدرات لتحويل اللغة العربية المنطوقة إلى نص قابل للبحث والتحليل.

من التدوين اليدوي إلى التدوين المؤتمت

تاريخيًا جرى تدوين نص المحادثات المُعترضة يدويًا. وقد أكد جنود سابقون أنه تم تكليف جنود إسرائيليين يهود تعلّموا اللغة العربية بالاستماع إلى المكالمات المسجلة وتدوين نصّها.[134] فيما يقوم جنود دروز أو جنود يهود من جذور سورية «الذين تعتبر اللغة العربية لغتهم الأم»، بمراجعة هذه النصوص،[135] علمًا أن معظم

130 فلسطين اليوم، «كيف تتنصّت المخابرات الإسرائيلية على جوالك الشخصي؟! فلسطين اليوم، 30 كانون الأول/ ديسمبر 2013، https://paltodaytv.com/post/466/كيف - -تتنصت-المخابرات-الإسرائيليةعلى-جوالك-الشخصي.

131 هناء صلاح، «البصمة الصوتية أداة اسرائيل لتنفيذ سياسة «التصفية الجسدية»، المونيتور، 4 شباط/ فبراير 2014، https://www.al-monitor.com/ar/contents/articles/originals/2014/02/gaza-israel-islamic-jihad-hamas-mobile-war.html.

132 ياسين جميل، «تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية»، رأي اليوم، 21 حزيران/ يونيو 2016، https://www.raialyoum.com/تفاصيل -مذهلة-عنطرق-وأساليبالمراقبة-ا.

133 AVG، البرمجيات الخبيثة لا تزال تتجسس عليك حتى عندما يكون هاتفك الخلوي مُعطلًا، 14 أيلول/ سبتمبر 2018، https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off.

134 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

135 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

ضباط الجيش اعترفوا في شهاداتهم أن مستوى اتقانهم للغة العربية «يصل إلى الصفر».[136] نظرًا إلى حجم بيانات التجسس الصوتي التي تلتقطها إسرائيل، صارت عمليات التنضيد والتدوين والترجمة تعتمد اليوم على الأنظمة المؤتمتة والآلية.

المنطق من وراء دمج أدوات التدوين القائمة على السحابة

إن استخدام نماذج Microsoft Azure - إلى جانب نماذج الشركات السحابية الأخرى - مصحوب أو من المحتمل أن يحل محل «نماذج اللغة الأصغر» التابعة للوحدة 8200 والقادرة على تدوين وترجمة اللغة العربية المنطوقة إلى العبرية.[137] أشارت مجلة 972+ إلى المناقشات الداخلية حول النقل إلى التخزين السحابي، حيث شدد القادة والضباط على ميزة الاستفادة من الخدمات السحابية المُدمجة بمجرد نقل بياناتهم إلى السحابة، نظرًا إلى القدرات التي يملكها مزودو الخدمات السحابية، «هم أيضًا لديهم قدرات STT [speech-to-text]. إنها جيدة؛ لديهم العديد من القدرات. لماذا علينا أن نطوّر كل شيء في الوحدة العسكرية، إذا كانت هذه القدرات قائمة أصلًا»؟[138]

يشرح خبراء سلاسل التوريد الخوارزمية بأنها جزء من نهج عمل مزوّدي الخدمات السحابية. تقدم هذه الشركات، كما هو الحال بالنسبة لمايكروسوفت، تقنيات الذكاء الاصطناعي الخاصة بها التي سبق وصُنعت، كخدمة «في مجالات مثل اللغة والكلام [...] والتحليلات»، إلى جانب قدرات التخزين السحابية الخاصة بها.[139] هناك عدد محدود من المؤسسات «القادرة على إنتاج أحدث تقنيات الذكاء الاصطناعي داخليًا».[140] ويرجع ذلك إلى وجود عوائق كبيرة على الولوج، بما في ذلك الوصول إلى «كميات كبيرة وذات صلة من البيانات، يحتمل أن تكون من مصادر متعددة، وقد تكون مصنفة أو خاضعة للإشراف، تُعنى بالعديد من السياقات، الاستخدامات، والمواضيع» بالإضافة إلى «خبرة شحيحة في تدريب نماذج واختبارها ونشرها، وكلها ذات احتياجات تخزين وحوسبة وشبكات كبيرة».[141] وبالتالي، تعرض شركات التقانة العملاقة أمثال مايكروسوفت وأمازون تقنيات الذكاء الاصطناعي القائمة على السحابة «بهدف موضعة نفسها استراتيجيًا في العديد من أشكال وأنواع الأسواق وسلاسل التوريد».[142]

إستخدام وظائف التدوين والترجمة المُسبق بناؤها من قبل أمازون ومايكروسوفت بالنسبة للبيانات الصوتية المخزنة في AWS، لا تؤكد المعلومات المتاحة للجمهور استخدام أدواتها للتنضيد والتدوين والترجمة. إلا أنه نظرًا للعوائق المذكورة آنفًا على الولوج، من المحتمل أن تكون الوحدة 8200 تستخدم Amazon Transcribe.[143] و Amazon Translate[144] لبيانات التجسس الصوتيّ التي تُخزّنها على AWS.

136 نكسر الصمت، حُكم عسكري: شهادات جنود من الإدارة المدنية، منسّق أعمال الحكومة في الأراضي المحتلة (نكسر الصمت، 2022)، 41، https://www.breakingthesilence.org.il/inside/wp-content/uploads/2022/07/Military_rule_testimony_booklet.pdf.

137 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

138 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

139 جينيفر كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، مؤتمر ACM 2023 حول المساءلة العادلة والشفافية، 12 حزيران/ يونيو 2023، 1188، https://doi.org/10.1145/3593013.3594073.

140 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1188.

141 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1188.

142 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1189.

143 Amazon Web Services, Speech to Text Service - Amazon Transcribe, n.d., https://aws.amazon.com/pm/transcribe/.

144 Amazon Web Services, Amazon Translate, n.d., https://aws.amazon.com/translate/.

أما بالنسبة للبيانات المُخزّنة على خوادم مايكروسوفت، كشفت أسوشييتد برس AP أن إسرائيل تستخدم أدوات Azure لتدوين وترجمة «المكالمات الهاتفية [...] والرسائل الصوتية» المخزنة في سحابة الشركة.[145] وفي حين أن الوثائق المُسرّبة التي راجعتها صحيفة «ذي جارديان» لا تأتي على ذكر الأدوات المحددة، تُشير في تقريرها إلى قيام «الجيش الاسرائيلي باستخدام أدوات Azure للترجمة وتحويل الكلام إلى نص القائمة على الذكاء الاصطناعي»،[146] وتشكل الترجمة «نحو نصف متوسط الاستهلاك الشهري».[147]

تتطابق هذه الميزات مع وصف Azure Speech من مايكروسوفت، والذي يتضمن، وفقًا لموقعها الإلكتروني، تحويل الكلام إلى نص، بما في ذلك تدوين الملفات الصوتية المسجلة مسبقًا بالإضافة إلى تدوين بدفعة واحدة لأحجام كبيرة من الملفات الصوتية.[148] وتشمل خصائص إضافية ذات صلة تحديد اللغة، تقييم النطق، وترجمة الكلام.[149] نظرًا لكل هذه القدرات - واستهلاك الجيش الإسرائيلي للذكاء الاصطناعي من Azure على نطاق واسع، يرجح الاستنتاج أن خدمات Azure Speech تستخدم لمعالجة البيانات الصوتية المستضافة في سحابة Azure.

4.3. تحليل الكلام

في حين أن التدوين والترجمة يحولان الصوت الخام إلى نص قابل للبحث والتحليل، من المُرجّح أن تنطوي الخطوة التالية في البنية التحتية للتجسس الصوتيّ الإسرائيلي على استخدام تحليل الكلام؛ علمًا أن تقارير إخبارية تُشير إلى أنها تشمل البحث عن كلمات دلالية، تعليم المُحتوى، تحليل روح الكلام، والتعرف على الأنماط.

البحث عن كلمات دلالية وتعليمها

إحدى الخصائص الأساسية لتحليل الكلام هي خاصية البحث عن الكلمات الدلالية. مما يتيح التعرّف على المحتوى ذي الصلة في كميات كبيرة من البيانات المُعترضة. وقد أشار ضابط استخبارات في حديثه لأسوشييتد برس AP، إلى استخدام Azure لاجراء بحث سريع عن مصطلحات مُحددة في نصوص «محادثات بين شخصين في ملف يبلغ طوله 50 صفحة».[150] بالإضافة إلى Azure، ذكرت مجلة 972+ أن الوحدة 8200 تستخدم نماذجها الأصغر لتصنيف وفرز المعلومات وإجراء «عمليات بحث فعالة عن الكلمات الدلالية» عبر بيانات التجسس الصوتيّ.[151]

كما نوّهت وكالة أسوشييتد برس AP الاخبارية إلى أن الجيش الإسرائيلي يقوم «بالتدقيق في مجموعة كبيرة من المعلومات الاستخباراتية والاتصالات المُعترضة

145 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

146 هاري ديفيز ويوفال أبراهام، «كشف: مايكروسوفت تعزز علاقاتها مع الجيش الإسرائيلي لتقديم الدعم الفني خلال حرب غزة»، ذي جارديان (القدس)، 23 كانون الثاني/ يناير 2025، https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.

147 يوفال أبراهام، «وثائق مسربة تكشف العلاقات العميقة بين الجيش الإسرائيلي ومايكروسوفت»، مجلة 972+، 23 كانون الثاني/ يناير 2025، https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/.

148 مايكروسوفت، ما هي خدمة الكلام ؟، 5 تشرين الثاني/ نوفمبر 2025، https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview.

149 مايكروسوفت، ما هي خدمة الكلام ؟

150 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

151 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».

ومحتوى التجسس لتحديد كلام أو سلوك مشبوه»،[152] إلا أن الأدوات المُحددة المُستخدمة لا تزال غير معلومة. يمكن إجراء هذا النوع من التعليم (وضع علامة) عبر عدة تقنيات متباينة، ولكن يُرجّح أنه يتم استخدام المسح التلقائي للنصوص البيانات الصوتية المُدوّنة بحثًا عن مصطلحات مُحددة.

وقد ثبت استخدام هذه القدرة سابقًا للرسائل النصية المكتوبة في نظام يسمى «الرسالة الصاخبة»، والذي طورته أيضًا الوحدة 8200 بعد 2015 ولا يزال قيد الاستخدام حتى يومنا هذا.[153] يجمع هذا النظام «رسائل الفلسطينيين النصية» ويُصنّف كل منها بموجب درجات «الخطورة».[154] وأكدت مصادر لصحيفة «ذي جارديان» أن التدريج المذكور يعتمد على مسح تلقائي (مؤتمت) لجميع الرسائل النصية بين الفلسطينيين في الضفة الغربية بحثًا عن كلمات يصنّفها الجيش الاسرائيلي كمشبوهة.[155]

تحليل روح الكلام

تحليل روح الكلام يُمكّن تحديد الحالات العاطفية أو النية في المُحادثات المُعترضة. وبالإمكان إجراء تحليل روح الكلام على الصوت ذاته (من خلال تحليل العلامات الصوتية مثل حجم الصوت أو ضيق الحبال الصوتية) وعلى النص المنصوص والمُدوّن (عبر تحليل كلمات دلالية وتقييم المحتوى). على الرغم من عدم تأكيد أي من النهجين قيد الاستخدام - إن لم يكن كليهما - تشير مصادر «ذي جارديان» إلى استخدام نماذج تحليل روح الكلام «لتحليل المُحادثات الهاتفية المُعترضة تلقائيًا من خلال التعرّف على فلسطينيين يُعبّرون عن الغضب».[156] قد تكون هذه القدرات مدعومة بنماذج لغوية أصغر قامت الوحدة 8200 بتطويرها، إلى جانب، أو بالإضافة إلى أدوات Azure القائمة على السحابة، والتي يجري تطويعها واستخدامها «موضعيًا»، مما يعني على خوادم الوحدة الخاصة، وفي هذه الحالة في بيئة منفصلة غير مرتبطة بالانترنت.[157]

تمييز الأنماط

هناك بعض المؤشرات على أن إسرائيل تستخدم «نموذجًا أساسيًا»[158] يسعى إلى «استيعاب كل ما جُمع تاريخيًا وكشف روابط وأنماط يصعب على الإنسان استنباطها بقدراته الذاتية».[159] لا تتوّفر تفاصيل إضافية حول هذا النموذج، ولكن أفيد أن خبراء القطاع الخاص الإسرائيليين ساهموا في تصميمه أثناء أداءهم الخدمة العسكرية الاحتياطية.[160]

نموذج لغة OpenAI من خلال Microsoft Azure

تُفيد تقارير أن الجيش الإسرائيلي يستطيع الولوج إلى موديل GPT-4 التابع لشركة

152 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/فبراير 2025.

153 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

154 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

155 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

156 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».

157 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

158 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».

159 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».

160 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».

OpenAI لـ «تحليل مليارات قطع معلوماتية، التعلم من الحالات السابقة، والرد على التعليمات المنطوقة والمكتوبة».[161] كشفت وثائق راجعتها مجلة 972+ أن الجيش الإسرائيلي يستهلك خدمات ذكاء اصطناعي على نطاق واسع من Azure، وأن ربع ما يستهلكه يُخصص لـ GPT-4.[162] وفي وقت ذكر متحدث باسم الشركة أن «OpenAI لا تملك شراكة معهم [الجيش الإسرائيلي]»،[163] باشرت مايكروسوفت بعرض موديلات OpenAI في إطار عروض Azure بعد استثمار مليارات الدولارات في الشركة. في الواقع، كشفت تقاري مجلة 972+، أنه بدءًا من آب/ أغسطس 2023، «يحصل الجيش الاسرائيلي على الولوج من منصة Azure بدلاً من الولوج مُباشرة عبر OpenAI»[164] . وتدل حقيقة أنه «يمكن الولوج إلى خدمات OpenAI التجارية فقط من خلال Azure» على ميل سلسلة التوريد الخوارزمية الأوسع حيث «يمكن الولوج إلى خدمات مقدمي الخدمات الخاصة بالذكاء الاصطناعي فقط [...] سحابة هذا المزوّد بالتحديد، بدلًا من الولوج إليها من خلال منافس.[165]

تتيح العمليات والتقنيات الموضحة أعلاه التعرّف على البيانات الصوتية، تدوينها، ترجمتها، مُعالجتها، وتحليلها على نطاق واسع. بمُجرد مُعالجة هذه المعلومات، يمكن الاستفادة منها لمجموعة متنوعة من التطبيقات.

5. تطبيقات للبيانات الصوتية

تشير المعلومات المتاحة للجمهور إلى أربعة تطبيقات أساسية للبيانات الصوتية بعد تحليلها ومُعالجتها: (1) تقديم تقارير مُباشرة إلى الوحدات العسكرية والاستخباراتية؛ (2) التكامل مع قواعد البيانات الأخرى من خلال دمج البيانات؛ (3) الاستخدام كمواد تدريبية لموديل لغوي كبير LLM؛ و(4) الاستخدام كمدخلات في نظام مؤتمت لتوليد الأهداف.

5.1. تقديم تقارير مُباشرة

يتمثل التطبيق الأساسي للبيانات الصوتية التي جرى مُعالجتها في التوزيع الفوري المباشر للنصوص المُترجمة إلى الوحدات العملياتية. حيث ذكرت «ميدل إيست آي» عام 2021 أنه «تتم ترجمة النصوص بعد تدوين المُحادثات وإرسالها إلى وحدات استخبارات الجيش والشاباك».[166] تؤكد تقارير حديثة سير العمل المذكور: يستطيع القادة «الولوج إلى المعلومات الاستخباراتية الأولية المترجمة إلى العبرية».[167] في الممارسة العملية، هذا يعني أن المحادثات الصوتية المُعترضة - التي يتم تدوين محتواها وترجمته - توّفر معلومات استخباراتية خام يتم توزيعها على الجيش الإسرائيلي ووكالات الأمن الداخلي.

161 أبراهام، «وثاق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».
162 أبراهام، «وثاق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».
163 أبراهام، «وثاق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».
164 أبراهام، «وثاق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».
165 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1191.
166 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».
167 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».

5.2. دمج البيانات

لا تزال المعلومات العمومية المُتاحة حول كيفية دمج بيانات التجسس الصوتيّ مع بيانات أخرى محدودة، لكن المصادر المُتوّفرة تشير إلى أنها تشكل جزءًا من مجموعة أوسع من قواعد البيانات. يرّجح أن يكون يوسي سارئيل، الرئيس السابق للوحدة 8200 والمهندس الرئيس لاستراتيجية الذكاء الاصطناعي، «قاد مشروعًا واسع النطاق وذي تمويل مُعتبر، وسّع التجسس الإسرائيلي على الفلسطينيين إلى حدٍ كبيرٍ ودمج قواعد بيانات استخباراتية متعددة».[168] بينما أنه لم يُشر إلى قواعد البيانات المُحددة التي يتم دمج البيانات الصوتية بها، إلا أنه يرشح من كتابات سارئيل اجراء تقاطع مرجعيّ لـ «المعلومات المرئية، البيانات الخلوية، جهات اتصال وسائل التواصل الاجتماعي، صور، وجهات اتصال الهاتف الخلوي»، وربما أكثر من ذلك،[169] مردداً توصيف إيليا زريق لطبقات إسرائيل من جمع بيانات التجسس الجماعيّ.[170]

تظهر أمثلة على دمج بيانات من هذا النوع في أحدث التقارير. وذكرت أسوشييتد برس AP أنه بالإمكان التحقق من صحة المعلومات المجموعة والمستحصلة من التجسس الجماعي «في وقت لاحق بواسطة اجراء تقاطع مع أنظمة الاستهداف الداخلية في إسرائيل والعكس صحيح».[171] وحسبما ورد فإن الأدوات القائمة على Azure «تعثر وتحدد أشخاصًا يعطون التوجيهات لبعضهم البعض»، والتي يمكن مقاطعتها مع الأنظمة العسكرية لتحديد الموقع لأجل تحديد مواقع محددة.[172] قد يلقي هذا التكامل بين البيانات الصوتية وتحديد الموقع الجغرافي الضوء على أداة صوتية للذكاء الاصطناعي غير مذكورة استخدمها الجيش الإسرائيلي في غزة لتحديد موقع قادة المقاومة، إذ أنها تُعطي موقعًا تقريبيًا للمكان الذي كانوا يجرون مكالمات هاتفية منه.[173]

5.3. بيانات التدريب لنموذج لغوي كبير

تُستخدم بيانات التجسس الصوتيّ أيضًا كمواد تدريبية لنموذج لغوي كبير (LLM) تعمل الوحدة 8200 على تطويره. كشف تحقيق أجرته «ذي جارديان» أن الوحدة تعمل على إنتاج نموذج لغوي كبير بهدف الاستفسار عن الاتصالات التي تعترضها من الفلسطينيين تحديدًا. توضح كمية بيانات التدريب المطلوبة لمثل هذا النموذج «المخزون الضخم من محتوى الاتصالات المُعترضة التي تحتفظ بها».[174] وعلى الأرجح أكثر بكثير من مُدة الاحتفاظ المُفترضة - نحو شهر.[175] يدعم «الاستوديو» هذا المشروع لإنتاج هذا النموذج اللغوي الكبير LLM مما يُشير إلى ارتباط الوحدة

168 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

169 هاري ديفيز وبيثان مكيرنان، «رئيس المخابرات الإسرائيلية يكشف هويته الحقيقية في زوال الأمن عبر الإنترنت»، ذي جارديان، 5 نيسان/ أبريل 2024، https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse.

170 زريق، «الاستعمار، التجسس، والتحكم بالمجتمعات»، 13-12.

171 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

172 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

173 شيرا فرينكل وتنان أودينهايمر، «اختبارات إسرائيل للذكاء الاصطناعي في حرب غزة تثير مخاوف أخلاقية»، نيويورك تايمز، 25 نيسان/ أبريل 2025، https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.

174 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».

175 ديفيز وأبراهام، «مليون مكالمة في الساعة «: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

8200 بخبراء القطاع الخاص من شركات أمثال ميتا، جوجل، مايكروسوفت، وشركات أخرى،[176] سعت الوحدة للحصول على مساعدتهم.[177]

وفقًا لأوري غوشين، الرئيس التنفيذي المشارك لشركة AI21 Labs الإسرائيلية المتخصصة في نماذج اللغة، والذي قدم المساعدة للوحدة 8200 هو الآخر، فإن النماذج اللغوية الكبيرة LLM مُفيدة نظرًا «لقدرتها على تجميع بيانات موّزعة في مصادر مُتعددة. عوضًا عن استخدام «أدوات البحث البدائية»، يستطيع الضباط بكل بساطة «طرح أسئلة وتلقي إجابات» من بوت المُحادثة».[178] يمكن الاستعلام عن بوت المحادثة، على سبيل المثال، حول «ما إذا كان شخصان قد التقيا من قبل».[179] في حين أنه بدأ تطوير النموذج اللغوي الكبير المذكور قبل أكتوبر 2023، بموجب تقارير،[180] إلا أن هذه العملية تسارعت أواخر 2024 بدعم إضافي من القطاع الخاص. لا يزال من غير الواضح ما إذا كان النموذج قد تم نشره واستخدامه بالفعل.[181]

التعليل العقلاني لاستخدام بيانات التجسس الصوتيّ لهذا النموذج اللغوي الكبير عوضًا عن النموذج الحالي واضح ومباشر. أمثلة للغة العربية الفلسطينية المنطوقة - سواء من نصوص المُكالمات أو مُحادثات واتس-أب نادرة عبر الإنترنت، خاصة «بالكمية اللازمة لتدريب مثل هذا النموذج».[182] غالبًا ما يجري تدريب النماذج العربية التجارية أو مفتوحة المصدر الحالية على اللغة العربية الفُصحى، وليس اللهجات المنطوقة التي يستخدمها الفلسطينيون بالحياة اليوميّة. لذلك جمعت الوحدة 8200 «جميع النصوص (العربية المنطوقة) المُدوّنة التي تملكها الوحدة» وأدخلتها في مستودع مركزي لاستخدامه كمجموعة بيانات تدريبية.[183] وبحسب مصادر تحدثت لصحيفة «ذي جارديان»، تتكوّن مجموعة البيانات هذه من نحو 100 مليار كلمة بالمُجمل، تغطي اللهجتين الفلسطينية واللبنانية. وعليه، فحتى حينما لم تكن للمُحادثات أي قيمة لأغراض استخباراتية عسكرية بحتة، عند اعتراضها، إلا أنها كانت قيّمة بالنسبة للوحدة 8200 لاستخدامها في تدريب وتحسين دقة نموذجها.

وقد أعلن الشاباك في 2023 عن إنشاء بوت مُحادثة منفصل ومُختلف عن ذاك الخاص بنموذج الوحدة 8200 اللغوي الكبير LLM، على أن يتم إدماجه على خوادم الوكالة.[184] ومع ذلك، من غير المعروف ما إذا كان بوت المُحادثة هذا يعتمد على بيانات التجسس الصوتيّ كبيانات تدريب.

176 تايمز أوف إسرائيل، «تقرير: إسرائيل تستخدم الذكاء الاصطناعي لتحديد موقع قادة حماس، والعثور على رهائن في أنفاق غزة».
177 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
178 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
179 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
180 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
181 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».
182 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
183 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».
184 يوفال مان وكورين إلباز- ألوش، «رئيس الشاباك رونين بار يقول إن الجهاز يطوّر أداة شبيهة بـ ChatGPT للكشف عن التهديدات»، YNet، 27 حزيران/ يونيو 2023، https://www.ynetnews.com/business/article/hjmohud002.

5.4. مُدخلات البيانات في خوارزمية توليد الأهداف العسكرية

أخيرًا، تُشير تقارير إلى أن البيانات الصوتية تُستخدم كأحد المُدخلات - إلى جانب مصادر البيانات الأخرى - في أنظمة توليد الأهداف المؤتمتة، وأبرزها تلك المعروفة باسم «لافندر».[185] تخصص «لافندر» للأفراد في غزة «درجة خطر» رقمية، وإذا كانت الدرجة أعلى من الحد الأدنى المُحدد، فهي تُعرّفهم كأهداف بشرية.[186] إلا أنه وكما تحذر هيومن رايتس ووتش، بدون إمكانية الدخول إلى اللافندر، من المستحيل أن نشير إلى أي من نقاط البيانات تساهم في تحديد هذه الدرجات بالكامل.[187]

ومع ذلك، هناك العديد من التقارير الإخبارية التي تشير إلى أن بيانات التجسس الصوتيّ تغذي خوارزميات توليد الأهداف مثل لافندر. وفقًا لمجلة 972+، ذكرت ثلاثة مصادر استخباراتية أنه تم توظيف مجموعة الاستخبارات السحابية التابعة للوحدة 8200 - والتي تحتوي على بيانات صوتية - خلال العامين الماضيين للتخطيط لغارات جوية مُميتة في غزة.[188] كما كشفت «ذي جارديان» أنه تم استخدام «المخزون العائل من المكالمات الهاتفية» المُخزّنة في Azure لتحديد أهداف القصف.[189]

تبعًا لمؤلفاتهما التي تناولت العنف اليومي للتجسس الإسرائيلي، توضح شلهوب - كيفوركيان وعثمان كيف تقوم أنظمة مثل لافندر «بتجريد الخاضعين للتجسس من إنسانيتهم وتهميشهم»، مما يختصر البشر بدرجات من الخطورة ويحرمهم من الاعتراف بإنسانيتهم.[190] من هذا المنظور، تُمسي البيانات الصوتية نقطة بيانات إضافية تستخدم لتصنيف الأهداف البشرية خوارزميًا، وتقييمها حسب درجات خطورة، واختيار الأهداف.[191]

6. قيود تقنيات الصوت الخوارزمية

يجمع جهاز التجسس الصوتيّ في إسرائيل بين مكونات أدوات تحويل الكلام إلى نص، والترجمة المدعومة بالذكاء الاصطناعي، والتعرّف على الصوت، والنماذج اللغوية الكبيرة - المُعرّضة للأخطاء وعدم الدقة التي يمكن أن تؤدي إلى سوء تعريف الأشخاص وسوء تفسير الكلام. تحمل إخفاقاتهم الفنية عواقب في العالم الحقيقي، بما في ذلك الاعتقالات غير المشروعة والاستهدافات المُميتة.

غالبًا ما تسيء أدوات التدوين والترجمة القائمة على الذكاء الاصطناعي تفسير الكلمات أو السياق. على سبيل المثال، تضمن أحد الأخطاء المُبلّغ عنها في نظام

185 يوفال أبراهام، «لافندر»: جهاز الذكاء الاصطناعي الذي يوّجه موجة القصف في غزة، 3 نيسان/ أبريل 2024، https://www.972mag.com/lavender-ai-israeli-army-gaza/.

186 هيومن رايتس ووتش، أسئلة وأجوبة: استخدام الجيش الإسرائيلي للأدوات الرقمية في غزة، 10 أيلول/ سبتمبر 2024، https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza.

187 هيومن رايتس ووتش، أسئلة وأجوبة: استخدام الجيش الإسرائيلي للأدوات الرقمية في غزة.

188 أبراهام، «مايكروسوفت تُخزّن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

189 ديفيز وأبراهام، «مليون مكالمة في الساعة «: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

190 شلهوب - كيفوركيان وعثمان، «السرية كعنف استعماري: حالة القدس الشرقية المحتلة»، 191.

191 سارة فتح الله، «الذكاء الاصطناعي والتحّكم بحياة وموت الفلسطينيين، مطبعة السياسة التقنية، 12 آب/ أغسطس 2025، https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/.

التجسس الصوتيّ في إسرائيل المصطلح العربي «الدفع» الذي تمت ترجمته بشكل خاطئ على أنه «القبضة على أنبوب الإطلاق لقذيفة صاروخية»، مما كاد يضع الأفراد على قوائم الأهداف بالخطأ.[192] كما واجه بوت المُحادثة الذي عمدت الوحدة 8200 إلى تطويره «صعوبة في التعرف على اللهجة العامية الحديثة والكلمات المُنقحرة أو المُحرفة من الإنجليزية».[193] إنه ليس بحالة شاذة، إذ تبيّن أن مُعدلات دقة التعرّف المؤتمت على الكلام باللغة العربية دون المستوى.[194] تباين اللهجات واللكنات ومخارج الحُروف تؤدي إلى مُضاعفات إضافية[195] وتفاقم سوء التفسير، كما يتضح من حالة تم فيها تصنيف لاجئ فلسطيني بشكل غير صحيح على أنه سوري بناءً على نطقه لمقطع واحد.[196] تتواصل هذه الأخطاء حتى عندما يُفترض أنه تتم مراجعة بشرية. قد يكتشف الضباط الناطقون بالعربية بعض الأخطاء،[197] إلا أن التحيّز التأكيدي[198] والعمل المُضاف[199] يُشير إلى أنه من المحتمل أن تمر أخطاء من دون تصحيح، أو قد يرغب القادة في تجاوز مراكز اللغة العسكرية والخبراء اللغويين تمامًا.[200]

بالإضافة إلى الترجمة، فإن «الهلوسة»- مُخرجات النموذج الخوارزمي التي ينتجها النموذج دون أساس في مادة المصدر - تفرض المزيد من المخاطر. معلوم أن نموذج OpenAI للترجمة Whisper وأدوات التدوين والترجمة الأخرى، إن كانت الوحدة 8200 توّظفها، تزيّف وتختلق النصوص، إلى جانب كونها «تُضيف تعليقات عنصرية وتستخدم خطابًا عنيفًا».[201] تعترف المصادر بأن «الاعتماد الأعمى على هذه الأدوات» مُحتمل،[202] مما يزيد من خطر تأثر القرارات بمعلومات مُختلقة حقيقة.

علاوة على ذلك، لتقنيات استخراج البصمة الصوتية معدلات تصنيف إيجابي خاطئ عالية،[203] كما أن تحليل روح الكلام الذي يستلزم التعرّف إلى العواطف والنوايا من كلام المرء يحظى باستنكار واسع كونه يفتقد للموثوقية،[204] مما يعكس كل من

192 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

193 تايمز أوف إسرائيل، «تقرير: إسرائيل تستخدم الذكاء الاصطناعي لتحديد موقع قادة حماس، والعثور على رهائن في أنفاق غزة».

194 فواز س. العنزي وضياء أبو زينة، «ملخص عن التعرف على الكلام العربي»، مجلة عين شمس الهندسية 13، رقم. 2 (2022): 101534، https://doi.org/10.1016/j.asej.2021.06.020.

195 دانيال ليكس بالومبو وروبرت بري، «سبر القياسات الصوتية البيومترية: مقارنة وتباين كيف تقوم الدولة والقطاع الخاص بتحديد الهُويّة من خلال الصوت»، البيانات الكبيرة والمجتمع 11، رقم. 4 (2024): 20539517241297889، https://doi.org/10.1177/20539517241297889.

196 كارين بيسترفيلد وآنا كفيكالوفا، «أصوات عدلية: ثقافات الكشف عن الصوت والتعرّف عليه في الغرب»، الدراسات الصوتية 9، رقم. 2 (2023): 156، https://doi.org/10.1080/20551940.2023.2232211.

197 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

198 مايكل بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025، https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.

199 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

200 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».

201 بيسيكر وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تنشأ مخاوف بشأن دور التكنولوجيا في قرار الحياة والموت»، 18 شباط/ فبراير 2025.

202 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».

203 جاي ستانلي، «حول إنشاء قواعد بيانات عملاقة للبصمات الصوتية»، اتحاد الحريات المدنية الأمريكي، 16 تشرين الأول/ أكتوبر 2014، https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases.

204 جيد ماكلين، «أليكسا، هل أنا سعيد؟ كيف يُخفق التعرّف على المشاعر القائم على الذكاء الاصطناعي»، جامعة نيويورك، 18 كانون الأول/ ديسمبر 2023، https://www.nyu.edu/about/news-publications/news/2023/december/alexa—am-i-happy—how-ai-emotion-recognition-falls-short.html.

القيود التقنية ومخاطر سوء تطبيق تحديد الهُوية البيومترية واستدلال العواطف والنوايا.

تُفاقم هذه المُخرجات بفعل كون بعض هذه الأدوات تعمل كـ«صناديق سوداء»، إلى جانب معرفة محدودة بكيفية توليد الأنظمة الخوارزمية للمُخرجات أو تقديم التوصيات، مما يمنع إمكانية تتبع كيفية الوصول إلى الاستنتاجات أو تصحيح الأخطاء. وبالرغم من ذلك، قد لا تكترث إسرائيل أصلًا لتقليل معدلات الخطأ، إذ ذكرت مصادر إسرائيلية أن «القضية الأكثر إلحاحًا ليست بالضرورة دقة هذه النماذج، بل تمكينها للاعتقالات على نطاق واسع». فبنظرهم الغاية الأهم هي مواصلة توسيع قائمة «المُشتبهين»،[205] مهما كانت درجة الدقة.

7. العواقب والتأثيرات على الفلسطينيين

للتجسس الصوتيّ الإسرائيلي آثار عميقة على الفلسطينيين، إذ أنه يصوغ ويبرمج الحياة اليومية من خلال الاتهام، التجريم، والعواقب المميتة. وتبقى هذه التأثيرات والعواقب مرتبطة بالسياق العسكري والقتالي الأوسع للاحتلال.

الاتهام والاعتقالات

تسهل بيانات التجسس الصوتيّ بشكل مباشر اعتقال الفلسطينيين. يُتيح النطاق المتسّع للتجسس المُعزز بقواعد البيانات الصوتية الضخمة التابعة للوحدة 8200، للقادة العسكريين تجميع قوائم كبيرة من المُشتبهين في جميع أنحاء البلدات الفلسطينية، مما يُسهم بوضوح في زيادة أعداد الاعتقالات.[206] بالإمكان تحديد عدد وتواتر الاعتقالات بشكل تعسفي، وفي بعض الأحيان، «يدور الحديث عن مجرد قائد فرقة يريد 100 اعتقال شهريًا في منطقته»، حسبما كشف أحد المصادر.[207] إن الحد الأدنى المنخفض جدًا للاشتباه بالشخص - غالبًا ما يكون غامضًا أو غير مدعوم بأدلة - يُتيح للسلطات الاسرائيلية تبرير الاحتجاز، الابتزاز، أو حتى القتل المستهدف بأثر رجعي، باستخدام البيانات الصوتية لإضفاء الشرعية على قراراتها. فكما أكد مصدر لصحيفة «ذي جارديان»: «عند حاجتهم باعتقال شخص من دون توّفر سبب وجيه للقيام بذلك، هذا هو المكان الذي يجدون فيه المُبرر»، في إشارة إلى بيانات التجسس الصوتيّ المخزنة على السحابة.[208] يُتوّقع أن يؤدي تطوير نموذج الوحدة 8200 اللغوي الكبير LLM إلى تجريم واعتقال الفلسطينيين، وبالتالي إلى استفحال البيانات التي تُشير إلى أن «نحو 50% من الفلسطينيين البالغين في الأراضي المحتلة قد تعرضوا للاعتقال في مرحلة ما من حياتهم».[209]

تخفيف وتجريم الكلام

يتسبب التجسس المنتشر على نطاق واسع على محادثات الفلسطينيين مناخًا من الرُعب والرقابة الذاتية.[210] «لإدراكهم أن ما يقولونه [...] قد يكون مُراقبًا طوال

205 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
206 ديفيز وأبراهام،»الجيش الإسرائيلي يكشف أنه أنشأ أداة تشبه ChatGPT باستخدام مجموعة واسعة من بيانات التجسس على الفلسطينيين».
207 أبراهام، «إسرائيل تطوّر أداة شبيهة بـ ChatGPT تقوم بتسليح التجسس على الفلسطينيين».
208 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.
209 زريق، المشروع الاستعماري الإسرائيلي في فلسطين، 163.
210 زريق، «الاستعمار، التجسس، والتحكّم بالسُكان»، 16.

الوقت»،[211] يمتنع الفلسطينيون عن التعبير السياسي أو يتجنبون التحدث بحرية كما يحلو لهم،[212] إذ أنهم يتوّقعون احتمال أن تُوظّف مُحادثاتهم كمواد مُدينة أو تحريضية.[213] قوانين التحريض الجارفة التي سنتها إسرائيل تجعل من توجيه تهمة التحريض للفلسطينيين أمرًا شائعًا، وتساهم في ردع وتكميم أفواه الفلسطينيين،[214] المناصرين، وبشكل خاص المدافعين عن حقوق الإنسان، خشية أن يُتهموا بالتحريض.[215]

يحمل هذا التأثير المُخفف للكلام، أبعادًا طارئة، بالذات حينما تكون الاتصالات مهمة في إتاحة الوصول إلى معلومات مفصلية وحيوية. على سبيل المثال، أوضح أحد مديري مستشفيات غزة، أن كونه يعي أنه تحت المراقبة الدائمة «يشوّه ويُضيّق عالمه» لدرجة أنه بات «يتجنب الاتصال بأخيه خشية أن يُسأل عما إذا كانت أي صواريخ قد أطلقت من المنطقة المحيطة أو ما إذا كان الإسرائيليون قد وصلوا إلى المنطقة، على أن يُسيء أي مُستمع خفيّ تفسير هذه الكلمات أو تشويه معانيها».[216] عليه، لا يكتفِ التجسس الصوتيّ بتقويض التعبير السياسي فحسب، بل إنه يمنع الفلسطينيين من البحث عن معلومات منقذة للحياة إزاء التحركات العسكرية أو ظروف السلامة أو الوصول للمساعدات الإنسانية.

عمليات القتل والاغتيالات

كما يمكن ربط التجسس الصوتيّ مُباشرة بالحصائل الدامية والمُميتة. إذا ما كان التجسس الصوتيّ يُوّظف فعلًا كمُدخلات لأنظمة توليد الأهداف المؤتمتة التابعة للجيش الاسرائيلي، ستكون هذه التداعيات كارثية أكثر بكثير.[217] أحد الأمثلة المأساوية التي أوردتها «لوس أنجيلس تايمز» هي حالة جُمانة، أم فلسطينية استشهدت في غارة جوية إسرائيلية مع توأمها البالغين من العمر 4 أيام في غزة، حيث يشتبه أفراد أسرتها وزملاؤها في أنها استُهدفت خطأً باستخدام الذكاء الاصطناعي وبيانات الهاتف. وقد قال صديق للعائلة: «لا مُبرر. بالمرّة»، مضيفًا أن «يملك الإسرائيليون كل هذه التكنولوجيا. يستهدفون بالذكاء الاصطناعي، ويضربون بناءً على البصمة الصوتية، وعلى إشارات الهاتف. ألا يستطيعون مراجعتها والتأكد منها؟ لماذا قصفوا واستهدفوا هذه الأسرة»؟[218]

بالمُجمل، يوضح التجريم، تخفيف الكلام، والاستهداف الدامي والمُميت، المخاطر والعواقب الجسيمة للتجسس الصوتي على الفلسطينيين، مما يجعل مقاومة هذه المنظومة والاعتراض عليها أكثر إلحاحًا.

211 زريق، «الاستعمار، التجسس، والتحكّم بالسُكان»، 17.

212 أُسيد صديقي، «تأثير مخيف»: التجسس الإسرائيلي الدائم للفلسطينيين»، الجزيرة، 8 أيار/ مايو 2023، https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians.

213 صوفيا جودفريند، «عندما يُشكّل حديث فلسطيني عن السياسة تحريضًا»، Jewish Currents، 15 أيلول/ سبتمبر 2021، https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.

214 جودفريند، توسيع التجسس الرقمي في القدس وعواقبه على حقوق الفلسطينيين، 9.

215 هيومن رايتس ووتش، برامج التجسس المستخدمة لاختراق أجهزة المدافعين عن حقوق الفلسطينيين.

216 مهاوش، «مُراقَب، مُتابَع، ومُستهدَف».

217 Sarah Fathallah, 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine', Public Humanities 2 (2026): e7, https://doi.org/10.1017/pub.2025.10113.

218 نبيه بولس، «ذهب لتسجيل ولادة أولاده التوأم. وعاد ليجهم قتلى في قصف إسرائيلي»، لوس أنجيلس تايمز، 14 آب/ أغسطس 2024، https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike.

8. السُبل المُحتملة للإعتراض

تتورط العديد من الجهات والهيئات في التجسس الصوتيّ على الفلسطينيين، مما يزيد تعقيد المُحاسبة والمساءلة على تداعياتها وآثارها على الفلسطينيين، ولكنه يخلق أيضًا العديد من السُبل للاعتراض والطعن عليها. تظهر نقاط الضغط هذه لأن العديد من الجهات والهيئات تستطيع الاعتراض والطعن على النظام البيئي للتجسس الصوتيّ - الموظفين والمستثمرين والحكومات الأجنبية ومنظمات المُجتمع المدني والصحافيين الاستقصائيين.

8.1. المُحاسبة المُجزّأة

عند النظر إلى بنية التجسس الصوتيّ ككل، يبدو أن العديد من الجهات الفاعلة تعمل بالتنسيق مع بعضها البعض. تشمل الجهات الفاعلة الأساسية في سلسلة توريد التجسس الصوتيّ والوحدات العسكرية والحكومية الإسرائيلية (مثل الوحدة 8200 والشاباك)، شركات التكنولوجيا الإسرائيلية الخاصة (مثل AI21 Labs و NSO)، ومقدمي الخدمات السحابية (أمثال مايكروسوفت وأمازون). ترى هيلغا طويل - الصوري أهمية خاصة في فهم علاقات القوة القائمة بالبُنى التحتية الرقمية، إذ أنه، بنظرها، عند تتبع «مسارات التجسس الرقميّ» تستطيع أن تدرك كيف «لاسرائيل أن تظهر في المساحات التي ستسيطر فيها على تلك العُقد وتمتلكها وتديرها».[219]

سلاسل التوريد القائمة على البيانات هي سلاسل توريد «ترتبط فيها الجهات الفاعلة بتدفق البيانات فيما بينها،[و] حيث تساهم العديد من الجهات الفاعلة في إنتاج تقنيات الذكاء الاصطناعي، نشرها، وتطوير خصائصها الوظيفية».[220] ما ينبثق من هذه الأعمال المُنسّقة هو ما يُطلق عليه خبراء التكنولوجيا اسم «مشكلة تعدد الأيادي».[221] تنبُع المُشكلة من الحقيقة أنه لا جهة فاعلة تتحرك وحيدة، تتحمل مسؤولية الأفعال التي تُساهم عدة جهات فاعلة فيها بطرائق مُختلفة. وبالتالي، تتوّزع المسؤولية عن إنتاج هذه الأنظمة على جهات شتى تعمل في نظام بيئي مُعقد، مما يجعل من الصعب «تحديد الجهة المسؤولة عن انتهاكات حقوق الإنسان بدقة»،[222] وبالتالي يجعل من المُحاسبة والمُساءلة مُجزأة إلى حدٍ كبير.

تعقّد السرية والضبابية مهمة استيعاب وتحديد كافة الجهات الفاعلة وأدوارها في سلسلة توريد التجسس الصوتيّ.[223] ترفض الوحدات العسكرية الإسرائيلية التعليق أو التعقيب على أفعالها وعملياتها، في حين تدعي شركات التقانة الأجنبية، وبينها مايكروسوفت، في تصريحات علنية، أنها لا علم لها بكيفية استخدام وتوظيف منصاتها - حتى عندما يؤكد موظفوها في الفروع المحلية والشركات التابعة عكس ذلك.[224] بالإضافة، في حين أن هُويّة بعض الشركات الإسرائيلية التي تشكل جزءًا من هذه المنظومة معروفة، كما هو الحال بالنسبة لـ NSO و AI21 Labs، فمن

219 طويل - الصوري، «خطوط الاتصالات ومسارات التجسس الرقمي الإسرائيلية»، 208.

220 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1186.

221 هيلين نيسنباوم، «المُحاسبة والمُساءلة في مجتمع محوسب»، أخلاقيات العلوم والهندسة 2، رقم 1 (1996): 25–42، https://doi.org/10.1007/BF02639315.

222 منظمة العفو الدولية، مجموعة أدوات المساءلة الخوارزمية (2025)، https://www.amnesty.org/en/latest/research/2025/12/algorithmic-accountability-toolkit/.

223 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

224 ديفيز وأبراهام، «مليون مكالمة في الساعة »: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

المُحتمل - ولربما على الأرجح - أن تكون شركات إضافية متورطة فيها. على سبيل المثال، فقد ساعدت شركة التكنولوجيا الإسرائيلية Comm - IT الجيش الإسرائيلي في نقل بياناته إلى منصات سحابية بعد إنشاء Google و Amazon لمراكز بياناتها الخاصة في إسرائيل، إلا أنه ليس واضحًا إذا لعبت دورًا في نقل بيانات التجسس الصوتيّ بالذات.[225] وتشير تقارير إلى تطوير شركات إسرائيلية خاصة لأشكال إضافية من التجسس الصوتيّ، بينها «توكا» (Toka)، الشركة المسؤولة عن تطوير أداة للتنصّت على السائقين من خلال ميكروفون سيارتهم، إلا أنه ليس واضحًا إذا تم استخدام هذه التقنية في صفوف الفلسطينيين.[226] بعبارة أخرى، قد تكون جهات أخرى في قطاع التقانة الإسرائيلي الخاص جزءًا من هيكلية التجسس الصوتيّ هذه، وإن لم تكن جميعها معروفة للجمهور.

ومع ذلك، رغم كون العديد من الجهات الفاعلة إحدى مُكوّنات سلسلة التوريد القائمة على البيانات، من الضروري ألا نُنكر أهمية ترتيباتها غير المتناسقة. بعض الجهات الفاعلة، وخاصة الجيش الإسرائيلي ومُزوّدي الخدمات السحابية، لها أهمية نسبية أكبر للمنظومة، في حين أن البعض الآخر قد يكمل بعض المهام الفرعية. تحتل الوحدة 8200 - والجيش الإسرائيلي بالعموم - موقعًا مركزيًا ككيان يبني أدوات ونماذج التحليل الصوتي، داخل مؤسساتها، وتجتذب دعم جهات أخرى، وتكتسب (أو تقتني) تقنياتهم، بالإضافة إلى مشاركة البيانات الصوتية معهم أو الحصول عليها منهم. لكن الخبراء يعترفون أيضًا بأن «مزودي الخدمات السحابية الرئيسيين الذين يتحكمون غالبًا في التقنيات الأساسية [يشغلون] مناصب مهمة عبر سلاسل التوريد في العديد من القطاعات».[227] في نهاية المطاف، «هذا التباين في الاعتماد المتبادل يُنتج تباين وعدم تماثل في السلطة»،[228] حيث تلعب الجهات الكُبرى بشكل منهجي دورًا أهم في تحمل المسؤولية عن نتائج سلسلة التوريد.[229] تملك شركات التكنولوجيا الكبرى، كونها تزوّد الخدمات بشكل مُباشر كما أسلفنا الذكر في هذا التقرير، كما الشركات المُستثمرة، المُستحوذة والداعمة للشركات الإسرائيلية المتورطة في بُنية إسرائيل للتجسس الصوتيّ - أمثال، Nvidia، التي تخوض مُحادثات للاستحواذ على AI21 Labs[230] المزيد من القوة في سلسلة التوريد بحُكم الأمر الواقع. عند إدانة القوة التي تحملها سلسلة توريد التجسس الصوتيّ هذه في مسائل الحياة والموت، من المهم الأخذ بالحسبان أصحاب القوة والسلطة والمسؤولية أكثر من غيرهم في هذه السلسلة.

8.2. جهات من المحتمل أن تتمكن من تفعيل الضغط

الموظفون في الشركات والضالعين في شؤونها الداخلية

قد يكون للموظفين في شركات التكنولوجيا درجة معينة من التأثير على تطوير، صيانة، وبيع تقنيات أرباب العمل. وقد ثبت أن نشاطية وحَراك الموظفين داخل مايكروسوفت كان محوريّ. نظمت الحملة بقيادة الموظفين تحت عنوان «No

225 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

226 «وسائل إعلام إسرائيلية: شركات إسرائيلية تحوّل سيارات متصلة بالانترنت إلى أدوات تنصّت»، The Palestine Chronicle، 18 شباط/ فبراير 2026، https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/.

227 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1187.

228 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1190.

229 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1192.

230 «تقرير: Nvidia تخوض مُحادثات مُتقدمة للاستحواذ على AI21 Labs الإسرائيلية مقابل نحو 3 مليار دولار»، 30 كانون الأول/ ديسمبر 2025، https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-2025-12-30/.

Azure for Apartheid» سلسلة من الاحتجاجات في مقر الشركة في الولايات المتحدة ومكاتبها، مُطالبين بوقف العقود التي تدعم الجيش الإسرائيلي.[231] كما يتمثل دور الموظفين بالعمليات الداخلية عندما يُقوم مصدر داخلي أو مُبلغ عن مخالفات بتسريب المعلومات الداخلية إلى الصحافيين والكشف عنها للجمهور، لأجل وضعها رهن التدقيق وتعريض الشركة للمُساءلة والضغط؛ ومن بين هذه الأمثلة، يمكن الاشارة إلى الكشف عن استخدام الوحدة 8200 خدمات Azure لتخزين بيانات التجسس الصوتيّ.[232]

المستثمرون وأصحاب الأسهم

يستخدم المستثمرون النفوذ المالي والحوكمة في الشركات التي يمتلكون أسهمها، غالبًا من خلال المقترحات الرسمية أو في التعامل المباشر مع قيادة الشركات. في تموز/ يوليو 2025، قدم ما لا يقل عن 60 مستثمرًا من مايكروسوفت - يملكون مُجتمعين أسهمًا بقيمة تزيد عن 80 مليون دولار، مُقترحًا لاجراء تقييم في العناية الواجبة المفروضة على مايكروسوفت في التزامات الشركة بحقوق الانسان، «في مواجهة مزاعم خطيرة بالتواطؤ في الإبادة الجماعية وغيرها من الجرائم الدولية».[233] على وجه التحديد، طلب المستثمرون من مايكروسوفت تقييم كيف تتم إساءة استخدام تقنيات الذكاء الاصطناعي والسحابة من قبل العملاء العسكريين «لاقتراف انتهاكات لحقوق الإنسان أو انتهاكات للقانون الإنساني الدولي»،[234] بعد أن كشفت التحقيقات عن دور الشركة في تخزين كميات طائلة من بيانات التجسس الصوتيّ على الفلسطينيين.

وفي كانون الأول/ ديسمبر 2025، أعلن صندوق الثروة السيادية النرويجي البالغة قيمته 2,1 تريليون دولار - الأكبر في العالم وأحد المساهمين الرئيسيين في «مايكروسوفت» - أنه سيدعم طلب مساهمي الشركة المطالبين «مايكروسوفت» بالإبلاغ عن اي مخاطر لانتهاكات حقوق الإنسان في بُلدان يوجد منها تخوّفات كبيرة لارتكاب مثل هذه الانتهاكات. على الرغم من عدم ذكر إسرائيل بالاسم أو حرفيًا، إلا أن الاقتراح طالب بالشفافية فيما يتعلق بكيفية تقييم «مايكروسوفت» للمخاطر من انتهاك حقوق الإنسان المنبثقة عن استخدام مُنتجاتها، وتقييم ما إذا كانت ضوابطها الداخلية تمنع الانتهاكات بشكل ناجع وفعّال.[235] بعد بضعة أيام في اجتماع أصحاب الأسهم والمساهمين السنوي لـ«مايكروسوفت»، حصلت هذه المقترحات المعنية بحقوق الانسان على زخم كبير من الأصوات، وأيدها أكثر من ربع الأسهم المصوّتة.[236]

مُنظمات المجتمع المدني والناشطين

تُوفّر المؤسسات غير الربحية، مُنظمات حقوق الانسان، مجموعات المُرافعة والمُناصرة، والنشطاء من القواعد الشعبية رقابة عامة حاسمة. وتشمل

231 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».

232 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

233 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

234 لاين موليت، «إجراء غير مسبوق من جانب المستثمرين يطالب مايكروسوفت بأجوبة على أنباء عن تورّطها في الإبادة الجماعية بغزة»، جمعية أصدقاء الخدمة الأمريكيين، 23 تموز/ يوليو 2025، https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide.

235 مايك لودفيغ، «مايكروسوفت معرضة للمحاسبة على دورها في مساعدة ارتكاب إسرائيل للإبادة الجماعية في غزة»، Truthout، 3 كانون الأول/ ديسمبر 2025، https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/.

236 تود بيشوب، «ملفات: مقترحات حقوق الإنسان تحظى بأكثر من 25% من الأصوات في اجتماع مساهمي مايكروسوفت»، GeekWire، 9 كانون الأول/ ديسمبر 2025، https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/.

استراتيجياتهم الحملات والالتماسات والاحتجاجات والنشر الإعلامي. على سبيل المثال، نظمت مجموعة ناشطة، Geef Tegengas (Push Back)، مُظاهرات على أسطح مراكز بيانات «مايكروسوفت» في هولندا، وحثت الموظفين على التوقف عن العمل و»ترك عملهم حتى تتم إزالة جميع الاستخبارات الإسرائيلية من الخوادم»،[237] في رد فعل على الأنباء القائلة إن الوحدة 8200 كانت تستخدم منصة Azure السحابية، ولا سيما مراكز البيانات في هولندا، لتخزين بيانات الفلسطينيين الصوتية المُعترضة.

الصحافيون الاستقصائيون

تلعب الصحافة الاستقصائية المستقلة دورًا مهمًا في الكشف عن الانتهاكات. التحقيقات الوحيدة التي أجرتها «مايكروسوفت» - أولها في أيار/ مايو 2025[238] وثانيها في أيلول/ سبتمبر من العام ذاته[239]- في علاقتها بالوحدة 8200 والضرر الذي تسببه للفلسطينيين أن نشرت «ذي جارديان» و»مجلة 972+» وغيرها من الصحف تقارير تُفصّل فيها كيف تُوظّف Azure لتخزين ومعالجة البيانات الصوتية للفلسطينيين. لا تؤدي الصحافة الاستقصائية إلى بيانات وردود فعل من الشركات فحسب، بل إنها تُعلم وتوّعي الجمهور أيضًا. في الواقع، تعتمد الكثير من المعلومات التي يقدمها هذا التقرير عن بنية التجسس الصوتيّ التي تستخدمها إسرائيل على نطاق واسع، على الكشوفات الصحفية.

الحكومات الأجنبية والهيئات الدولية

تستطيع الحكومات الوطنية والهيئات الدولية تفعيل الضغط على الجهات الفاعلة في منظومة التجسس الصوتيّ من خلال السياسة التجارية أو العقوبات أو الإجراءات القانونية. على سبيل المثال، ناقشت الدول الأوروبية تدابير لمنع استخدام مراكز بيانات الاتحاد الأوروبي لاستضافة بيانات التجسس الصوتيّ، في حين أثار المقرر الخاص للأمم المتحدة احتمال تواطؤ الشركات في الجرائم الدولية، والتي يمكن أن تكون أسبابًا للتحقيقات والملاحقات القضائية من قبل المحكمة الجنائية الدولية والهيئات القضائية الوطنية.[240]

8.3. المطالب ومسارات العمل المحتملة

تعليق العقود أو إلغائها

غالبًا ما تنطوي المطالب المباشرة على تعليق أو إنهاء العقود، وفي الحالة التي نتناولها، نقصد تلك التي تكمن وراء بنية التجسس الصوتيّ في إسرائيل. في «قرار استثنائي»، قامت «مايكروسوفت» في نهاية المطاف «بإيقاف وتعطيل مجموعة من الخدمات لوحدة داخل وزارة الأمن الإسرائيلية»، بما في ذلك التخزين السحابي وخدمات الذكاء الاصطناعي، عُقب ضغط مُشترك من الموظفين والمستثمرين

237 هاري ديفيز، «نشطاء في هولندا يحتجون على سطح مبنى تابع لمايكروسوفت تستخدمه لتخزين البيانات العسكرية الإسرائيلية»، ذي غارديان، 10 آب/ أغسطس 2025، https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data.

238 مايكروسوفت، «بيان مايكروسوفت حول القضايا المتعلقة بخدمات التكنولوجيا المُقدمة في إسرائيل وغزة»، مايكروسوفت حول القضايا، 15 آب/ أغسطس 2025، https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/.

239 براد سميث، «تحديث حول مراجعة مايكروسوفت الجاري»، مايكروسوفت حول القضايا، 25 أيلول/ سبتمبر 2025، https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/.

240 مكتب المفوّض السامي لحقوق الإنسان، من اقتصاد الاحتلال إلى اقتصاد الإبادة الجماعية: تقرير المقرر الخاص المعني بحالة حقوق الإنسان في الأراضي الفلسطينية المُحتلة منذ عام 1967، https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur، A/HRC/59/23 (2025).

وتقارير صحافية استقصائية.[241] شكّل هذا القرار سابقة جديدة، حيث أن هذا «الانهاء للعقود، هو أول حالة معروفة لشركة تكنولوجيا أمريكية تسحب الخدمات المقدمة للجيش الإسرائيلي» منذ تشرين الأول/ أكتوبر 2023.[242] ومع ذلك، بالنسبة للبعض، لم تكن هذه سوى الخطوة الأولى من بين عدّة. في يوم الإعلان ذاته، دعت منظمة «No Azure For Apartheid» شركة «مايكروسوفت» إلى قطع جميع علاقاتها مع إسرائيل.[243] وبعد ذلك بوقت قصير، طالبت مجموعة من جماعات ومؤسسات حقوق الإنسان أيضًا بخطوات إضافية من شركة «مايكروسوفت»، موّجهة للمُدير التنفيذي للشركة باقة من الأسئلة: «ما هي الخطوات، إذا ما كانت ستُتخذ، التي ستتخذها [الشركة] لتعليق أعمالها وتعاملاتها مع الجيش الإسرائيلي والهيئات الحكومية الأخرى على خلفية وجود أدلة عن مساهمة هذه الأعمال التجارية في الانتهاكات الجسيمة لحقوق الإنسان ولارتكاب جرائم دولية»،[244] مطالبين بمُحاسبات ومُساءلات واتخاذ إجراءات إضافية.

المسؤولية القانونية

وإن كانت الدعاوى القضائية لم تسفر عن أثر محسوس في الماضي، إلا أن زريق يعتبر الترافع في هذه القضايا مُحبذًا، وذلك بفضل «الاهتمام المتزايد باحتمال قدرة حقوق الإنسان والقضايا العابرة للحدود التأثير على سياسات الدول وتحريك وتعبئة مجتمعات اللاجئين». فبنظره، الترافع بالقضايا في أروقة المحاكم قد أثبت «فعاليته في تعميم سوء معاملة المجموعات المُهمشة والمُستضعفة التي لا تملك أي سبيل آخر لرفع مظالمها من خلال أجهزة الدولة القومية».[245] قد تتعرض الشركات التي تستضيف بيانات التجسس الصوتيّ في الخارج للمسؤولية القانونية بموجب المجموعة القانونية لولاياتها القضائية المواتية، مما يتطلب من الشركات الامتثال لشروط محددة لضمان العناية الواجبة بحقوق الإنسان والالتزام بالأحكام القانونية لحماية البيانات والخصوصية. أثيرت هذه النقطة في رأي قانوني داخلي من وزارة القضاء الإسرائيلية عام 2022، والذي «أشار إلى أن كل من فرنسا وألمانيا تطلبان من الشركات التحقق من انتهاكات حقوق الإنسان في سلاسل التوريد الخاصة بها بموجب القانون»، مضيفًا أنه «إذا تم الكشف عن أن هذه الشركات تنشط في الأراضي الفلسطينية المحتلة، فإن مثل هذه القوانين قد تؤدي إلى إصدار أوامر لمنع أو تقييد الخدمات».[246] وفيما يتعلق ببيانات التجسس الصوتيّ المُخزّنة في مراكز بيانات Azure في هولندا، حذرت الوزارة من أن «هولندا تعمل على تشريع مماثل»، معربة عن قلقها من أن «دعوى قضائية محتملة ستسبب ضررًا لاسرائيل بشكل خاص».[247]

مخاوف وزارة القضاء الإسرائيلية ليست عديمة الأساس بالكامل. فقد أدت التقارير التي كشفت اعتماد الجيش الإسرائيلي على مراكز البيانات في هولندا لتخزين بيانات التجسس الصوتيّ إلى مُساءلات واستجوابات برلمانية، مما اضطر وزير الخارجية

241 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».

242 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».

243 No Azure For Apartheid، سقط حجر الدومينو الأول - مايكروسوفت تقطع بعض الخدمات المقدمة للوحدة 8200 الإسرائيلية، 25 أيلول/ سبتمبر 2025، https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b.

244 Access Now وآخرين، «يجب أن تكون مايكروسوفت واضحة بشأن دورها في حرب إسرائيل على غزة»، 10 تشرين الأول/ أكتوبر 2025، https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/.

245 زريق، المشروع الاستعماري الإسرائيلي في فلسطين، 47.

246 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

247 أبراهام، «مايكروسوفت تخزن معلومات استخباراتية إسرائيلية تستخدم لمهاجمة الفلسطينيين».

الهولندي للرد قائلًا: «إذا كانت هناك مؤشرات جديّة على جرائم جنائية بحسب تلك المعلومات، فيمكن بالطبع بدء اتخاذ اجراءات قضائية، نترك المسألة بأيدي النيابة العامة».[248] في أيرلندا، طلب المجلس الأيرلندي للحريات المدنية رسميًا من لجنة حماية البيانات الأيرلندية التحقيق مع «مايكروسوفت» بسبب «المعالجة غير القانونية» لبيانات الفلسطينيين الصوتية، في «خرق لأنظمة ولوائح الاتحاد الأوروبي لحماية البيانات (GDPR) التي تحكم استخدام البيانات الشخصية».[249]

تستطيع اسرائيل تجنّب وتخفيف المخاوف من مواجهة دعاوى قضائية من خلال الاحتفاظ ببيانات التجسس الصوتيّ في أطر خاضعة لولايتها القضائية. إذ أن مزوّدي الخدمات السحابية الرئيسيين أنشأوا مراكز بيانات خاصة بهم في إسرائيل. وقد قال مصدر لمجلة 972+ أنه من شأن هذا الأمر تذليل المخاوف من إجراءات قانونية في محاكم بالخارج.[250] هذا التكتيك شائع في سلاسل التوريد الخوارزمية، حيث تستخدم الجهات الفاعلة أي «استراتيجية تقنية قانونية» تساعدها على تقليل المخاطر، وفي حالة سلاسل التوريد العابرة للحدود، فهي تستفيد من المراجحة التنظيمية.[251] كما تستطيع إسرائيل أن تطلب التعاون من شركات التكنولوجيا، إذ تنصّ العقود مع شركات كأمازون وجوجل على وجوب إرسال رمز سري إلى إسرائيل لإبلاغها «عندما تكشف عن بيانات إسرائيلية إلى محاكم أو محققين أجانب»، بهدف «تفادي الأوامر القانونية».[252] مما يُتيح لاسرائيل نقل بياناتها على جناح السرعة، كما كان الحال في شأن البيانات التي خزّنتها في مراكز Azure للبيانات في هولندا، أيام قليلة بعد نشر تحقيق «ذي جارديان»،[253] ما اعتبره المجلس الأيرلندي للحريات المدنية أقرب إلى إخفاء «أدلة على المعالجة غير القانونية قبل بدء التحقيقات داخل الاتحاد الأوروبي».[254]

قد يكون التورط في سلسلة توريد التجسس الصوتيّ خرقًا للقوانين المحلية الأجنبية، وكذلك للقانون الدولي. وبصفتها ائتلافًا دوليًا لمجموعات حقوقية والمرافعة للحقوق - مركز القانون المناهض للعبودية، ومؤسسة آفاز Avaaz، والمركز الأوروبي للدعم القانوني، و SOMO، ومركز الحقوق الدستورية، وإيكو، و GLAN (شبكة الإجراءات القانونية العالمية) - حذرت هذه المؤسسات شركة مايكروسوفت في إشعار من التعرض للمسؤولية القانونية لتوّرطها في انتهاكات جسيمة لحقوق الإنسان، بما في ذلك «التجسس الإسرائيلي غير القانوني وواسع النطاق والقامع للسكان الفلسطينيين». فقد عرّضت شركة مايكروسوفت، بحسب الإشعار، «نفسها وقيادتها ومسؤوليها كأفراد، للمساءلة القانونية الجنائية والمدنية إلى حدٍ كبير، قابل للمحاكمة في المحاكم المحلية في الولايات المتحدة والاتحاد الأوروبي، وأمام مختلف الهيئات الدولية»،[255] كمحكمة الجنايات الدولية.

248 ديفيز، «نشطاء في هولندا يحتجون على سطح موقع لمايكروسوفت يُستخدم لتخزين البيانات العسكرية الإسرائيلية».

249 أوكارول، «مُطالبة السلطات الأيرلندية التحقيق مع مايكروسوفت إزاء مُعالجة مزعومة غير قانونية للبيانات من قبل الجيش الإسرائيلي».

250 أبراهام، «طلبية من أمازون»: كيف يُخزّن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

251 كوب وآخرون، «فهم المساءلة في سلاسل التوريد الخوارزمية»، 1194–95.

252 هاري ديفيز ويوفال أبراهام، «كشف: إسرائيل طالبت غوغل وأمازون باستخدام «غمزة « سرية لتجنب الأوامر القانونية»، ذي جارديان، 29 تشرين الأول/ أكتوبر 2025، https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.

253 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجيتها في التجسس الجماعي على الفلسطينيين».

254 أوكارول، «مُطالبة السلطات الأيرلندية التحقيق مع مايكروسوفت إزاء مُعالجة مزعومة غير قانونية للبيانات من قبل الجيش الإسرائيلي».

255 مركز القانون المناهض للعبودية، «دور مايكروسوفت المُساند للإبادة الجماعية التي ترتكبها اسرائيل ضد الفلسطينيين تعرض الشركة وقيادتها للمُساءلة القانونية»، مركز القانون المناهض للعبودية، 2 كانون الأول/ ديسمبر 2025.

تستطيع الدول التي تعترف باختصاص وصلاحية محكمة العدل الدولية أن ترفع دعاوى قانونية على الشركات العاملة تحت ولايتها القضائية (في إطار الدولة) إذا ما قضت المحكمة في النهاية بأن الحملة العسكرية هي إبادة جماعية.[256] يُوّفر القانون الإنساني الدولي وقانون حقوق الإنسان سُبلًا للطعن والاستئناف، والتقاضي أمام هيئات محكمة دولية ودعاوى قضائية عبر الحدود، على أساس انتهاك الحقوق الأساسية مثل الحق في الخصوصية وحرية التعبير والحق بالوصول إلى الإنترنت.[257] بموجب اتفاقيات أوسلو، يمكن أيضًا الادعاء بأن ذلك ينتهك حق السيادة الفلسطينية على البنية التحتية لتكنولوجيا المعلومات والاتصالات.[258]

العقوبات وضوابط التصدير

تستطيع الحكومات فرض عقوبات هادفة ومُحددة، أو فرض ضوابط على التصدير، أو إدراج الشركات التي تُمكّن انتهاكات حقوق الإنسان في القائمة السوداء، كالشركات المتورطة في منظومة التجسس الصوتيّ الإسرائيلي. إحدى هذه الأمثلة قيام الحكومة الأمريكية بإدراج شركات برامج التجسس NSO Group و Candiru في القائمة السوداء.[259] كما تستطيع الحكومات أيضًا فرض ضوابط على الصادرات. ومع ذلك، فإن هذا الأمر معقد بسبب طبيعة «الاستخدام المزدوج» للتقنيات المستخدمة في التجسس الصوتيّ، والتي يمكن استخدامها للأغراض العسكرية وغير العسكرية على حد سواء. على سبيل المثال، «صُنعت ضوابط الولايات المتحدة للصادرات أصلًا لتنظيم المواد ذات المدخلات العسكرية الواضحة وحالات الاستخدام»، لكن التقنيات ذات الاستخدام المزدوج التي تحمل أيضًا تطبيقات تجارية «يصعب تنظيمها على المستويين الوطني والدولي».[260]

تخلق المساءلة المجزأة وديناميكيات القوة غير المتكافئة للنظام البيئي الخاص بالتجسس الصوتيّ في إسرائيل نقاط ضغط متعددة لتحدي عملياتها، من نشاطية الموظفين وضغط المستثمرين إلى الإجراءات القانونية والملاحقة الدولية. في حين أن سابقة وقف مايكروسوفت تقديم الخدمات للوحدات العسكرية الإسرائيلية هي خير دليل على الجهود المُنسّقة للطعن على أنشطتها، إلا أن المُطالبات بمزيد من المساءلة واتخاذ إجراءات أقوى وذات فاعلية أكبر تؤكد أنها ليست إلا محض خطوة أولى في صراع أوسع. في نهاية المطاف، فإن الطبيعة المتنازع عليها لهيكل المراقبة هذا - التي كشفتها الصحافة الاستقصائية والضغط المُنظم والقانوني والعام - توّفر مسارات لتعطيل الأنظمة التي تمكن التجسس الصوتيّ الخوارزمي الإسرائيلي على الفلسطينيين.

256 ريان جريم ووقاس أحمد، «وثائق مُسرّبة: الجيش الإسرائيلي هو واحد من أفضل عملاء مايكروسوفت في شأن الذكاء الاصطناعي»، Drop site، 23 كانون الثاني/ يناير 2025، https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.

257 عنان أبو شنب، انقطاع الاتصال: سيطرة إسرائيل على البنية التحتية لتكنولوجيا المعلومات والاتصالات الفلسطينية وتأثيرها على الحقوق الرقمية (حملة – المركز العربي لتطوير الإعلام الاجتماعي، 2018)، 27، https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.

258 عبد الله وبحور، تكنولوجيا المعلومات والاتصالات: المُحرك المُقيّد المقيد لتنمية فلسطين.

259 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمة هاتفية في الضفة الغربية وغزة».

260 هانا كيلي، «التكنولوجيا مزدوجة الاستخدام وضوابط الصادرات الأمريكية، مختبر سياسة تكنولوجيا CNAS، 15 حزيران/ يونيو 2023، https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.

الخُلاصة

يستعرض تقرير «أصوات أسيرة» الانتهاك العميق الكامن في قلب التجسس الصوتيّ الإسرائيليّ الخوارزميّ الجماعيّ: الاستيلاء المنهجي على كلام ومُحادثات الفلسطينيين كآلية لقمعهم. أظهرت الفصول السابقة أن منظومة التجسس الصوتيّ المُطبقة على الفلسطينيين لا تعمل في فراغ وليست برنامجًا منفصلاً أو معزولًا، وبل إنها منظومة كثيفة، متعددة الطبقات، تهدف لالتقاط المُحادثات، تخزينها، تحليلها، وتوظيفها في العمليات. ما يظهر هو بنية تحكم يتم فيها تضمين البيانات الصوتية - وهو أثر حميم سريع الزوال للحياة اليومية - في مشروع أوسع للسيطرة على السُكان، متصل بأنماط أخرى من التجسس الجماعي الإسرائيلي. تؤثر بنية التجسس الصوتيّ هذه بعمق على الحياة الفلسطينية: تقييد التواصل، وإنتاج الخوف، وتسهيل التجريم، والاعتقالات، والموت.

حتى في إطار هيكلية وبنية السيطرة الرقمية هذه، هناك مسارات للاعتراض عليها والطعن فيها. لا يكشف التجسس الصوتيّ المنهجي للفلسطينيين عن حجم الاحتلال العسكري الإسرائيلي فحسب، بل يكشف أيضًا عن الدور المحوري للشركات وشركات التكنولوجيا ومقدمي الخدمات السحابية، الذين يمكن الضغط عليهم جميعًا من خلال وسائل مختلفة. تُظهر على سبيل المثال، حالة مايكروسوفت وحالات أخرى، أن الجهات الفاعلة في هذه المنظومة ليست مُكرّسة ولا ثابتة: تحت ضغط مستمر من العمال والمستثمرين وأصحاب الأسهم والصحافيين والمجتمع المدني والحكومات؛ بالإمكان إجبارها على تجميد أو تعليق العقود، أو تعديل الممارسات أو مواجهة تواطئهم في انتهاكات حقوق الإنسان.

ومع ذلك، فإن الطعن في منظومة التجسس الصوتي المذكورة يعني أيضًا التصدي للعقلية الاستعمارية والمنطق السرطاني التوّسعي الذي جعل مثل هذه المنظومة أصلًا قابلة للتصوّر والتطبيق. دون معالجة هذه الهياكل الأساسية - بما في ذلك تطبيع التجسس الجماعيّ وجمع البيانات، والاستثناء القانوني المُطبق في حالة الفلسطينيين، إلى جانب الحوافز الدبلوماسية والسوقية العالمية التي تكافئ صناعة الأمننة الإسرائيلية - تكمن مخاطرة في أن تُعيد جهود الإصلاح إنتاج المنطق الذي يسعون إلى إلغاء مفعوله.

ربما الوقائع المعروضة هنا ليست إلا غيض من فيض أو لمحة عن منظومة التجسس الصوتيّ الأكبر والأكثر غموضًا، لكنها ترسم خريطة أولية تعرّفنا على أساليب اعتراض البيانات الصوتية للفلسطينيين ومعالجتها وتسليحها. في نهاية المطاف، يُشكّل هذا المقال وثيقة ودعوة: دعوة لمزيد من البحث والتدقيق الأوسع والعمل المنسق - كل التدخلات التي يجب أن تظل قائمة على النضال الأوسع من أجل حقوق الإنسان والكرامة وتقرير المصير للفلسطينيين.

المراجع:

- 7amleh. Aš-Šabāb al-Filisṭyniyn Wa-Lmušārka Ās-Syāsya ʿabra Šabakāt at-Ttawāṣul ā-L'ijtimāʿy الشباب الفلسطينيين والمشاركة السياسية عبر شبكات التواصل الاجتماعي [Palestinian Youth and Political Participation via Social Media Networks]. 7amleh – The Arab Center for the Advancement of Social Media, 2019. https://7amleh.org/wp-content/uploads/2019-1استطلاع-حملة/10/.pdf.
- 7amleh. Facial Recognition Technology and Palestinian Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2020. https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights.
- 7amleh. Gaza Telecommunications Infrastructure: Assessment to Damages and Humanitarian Impact. 7amleh – The Arab Center for the Advancement of Social Media, 2024. https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en.
- 7amleh. Intensification of Surveillance in East Jerusalem Since October 2023. 7amleh – The Arab Center for the Advancement of Social Media, 2024. https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en.
- 7amleh. Netanyahu Imposes Dangerous "Big Brother" Surveillance under the Pretext of a Security Response to the Coronavirus. 23 March 2020. https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response.
- Abdullah, Wassim F., and Sam Bahour. ICT: The Shackled Engine of Palestine's Development. Al-Shabaka, 2015. https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.
- Abolitionist Law Center. 'Microsoft's Aiding of Israel's Genocide Against Palestinians Exposes Company and Its Leadership to Legal Liability'. Abolitionist Law Center, 2 December 2025.
- Abraham, Yuval. 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'. +972 Magazine, 6 March 2025. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.
- Abraham, Yuval. 'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza. 3 April 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.
- Abraham, Yuval. 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'. +972 Magazine, 23 January 2025. https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/.
- Abraham, Yuval. 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'. +972 Magazine, 6 August 2025. https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/.
- Abraham, Yuval. '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'. +972 Magazine, 4 August 2024. https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/.
- AbuShanab, Anan. Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2018. https://7amleh.org/wp-content/uploads/201901//Report_7amleh_English_final.pdf.
- Access Now, Amnesty International, Electronic Frontier Foundation, Human Rights Watch, 7amleh, and Fight for the Future. Microsoft Must Come Clean on Its Role in Israel's War on Gaza. 10 October 2025. https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/.
- Al Jazeera. 'Al-Duwairi: Al-Āḥtilāl Yastẖdim Baṣmaẗ al-Ṣūt Wāl'īn Litʿqwb Muqātilī al-Muqāwama Biġaza الدويري: الاحتلال يستخدم بصمة الصوت والعين لتعقّب مقاتلي المقاومة بغزة [Al-Duwairi: The Occupation Uses Voice and Eye Scans to Track Resistance Fighters in Gaza]'. Al Jazeera, 15 April 2025. https://www.aljazeera.net/news/2025الصوت-بصمة-يستخدم-الاحتلال-الدويري/15/4/.
- Al Jazeera. 'US Court Bars Israeli Spyware Firm from Targeting WhatsApp Users'. Al Jazeera, 18 October 2025. https://www.aljazeera.com/news/202518/10//us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users.
- Al Jazeera. 'What Is Project Nimbus, and Why Are Google Workers Protesting Israel Deal?' Al Jazeera, 23 April 2024. https://www.aljazeera.com/news/202423/4//what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal.
- Al-Anzi, Fawaz S., and Dia AbuZeina. 'Synopsis on Arabic Speech Recognition'. Ain Shams

Engineering Journal 13, no. 2 (2022): 101534. https://doi.org/10.1016/j.asej.2021.06.020.

- Ali, Rabia. 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?' Anadolu, 30 April 2024. https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563.
- Al-Jaafari, Wajdi. '"Mas'ūlūn: jamy' wasā'il al'ittiṣāl fī falasṭīn murāqaba" مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]'. Ma'an News Agency, 20 December 2014. https://www.maannews.net/news/748592.html.
- Alshurafa, Mohammed. The Impact of the Gaza Blockade and the Destruction of Telecommunications Infrastructure on the Digital Economy Amidst Genocide. 7amleh – The Arab Center for the Advancement of Social Media, 2025. https://7amleh.org/post/gaza-digital-economy-collapse-en.
- Amazon Web Services. Amazon Translate. n.d. https://aws.amazon.com/translate/.
- Amazon Web Services. Speech to Text Service - Amazon Transcribe. n.d. https://aws.amazon.com/pm/transcribe/.
- Amnesty International. Algorithmic Accountability Toolkit. 2025. https://www.amnesty.org/en/latest/research/202512//algorithmic-accountability-toolkit/.
- Amnesty International. Amnesty International and More than 170 Organisations Call for a Ban on Biometric Surveillance. 7 June 2021. https://www.amnesty.org/en/latest/press-release/202106//amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.
- Amnesty International. Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. 8 November 2021. https://www.amnesty.org/en/latest/research/202111//devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.
- AVG. Malware Is Still Spying on You Even When Your Mobile Is Off. 14 September 2018. https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off.
- Barghuthy, Eyad, and Alison Carmel. Silenced Networks: The Chilling Effect among Palestinian Youth in Social Media. 7amleh – The Arab Center for the Advancement of Social Media, 2019. https://7amleh.org/post/silenced-net-the-chilling-effect-among-palestinian-youth-in-social-media.
- Batniji, Rajaie. 'Searching for Dignity'. The Lancet 380, no. 9840 (2012): 466–67. https://doi.org/10.1016/S014061280-(12)6736-X.
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News, 18 February 2025. https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News (Tel Aviv), 18 February 2025. https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.
- Biggar, Paul. Meta and Lavender. 16 April 2024. https://blog.paulbiggar.com/meta-and-lavender/.
- Bijsterveld, Karin, and Anna Kvicalova. 'Forensic Voices: Cultures of Sonic Detection and Identification in the West'. Sound Studies 9, no. 2 (2023): 155–65. https://doi.org/10.108020551940.2023.2232211/.
- Bishop, Todd. 'Filing: Human Rights Proposals Win More than 25% of Votes at Microsoft Shareholder Meeting'. GeekWire, 9 December 2025. https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/.
- Breaking the Silence. Military Rule: Testimonies of Soldiers from the Civil Administration, Gaza DCL and COGAT. Breaking the Silence, 2022. https://www.breakingthesilence.org.il/inside/wp-content/uploads/202207//Military_rule_testimony_booklet.pdf.
- Bulos, Nabih. 'He Went to Register the Birth of His Twins. He Returned to Find Them Killed in an Israeli Strike'. Los Angeles Times, 14 August 2024. https://www.latimes.com/world-nation/story/202414-08-/four-day-old-twins-israeli-airstrike.
- Cobbe, Jennifer, Michael Veale, and Jatinder Singh. 'Understanding Accountability in Algorithmic Supply Chains'. 2023 ACM Conference on Fairness Accountability and Transparency, 12 June 2023, 1186–97. https://doi.org/10.11453593013.3594073/.
- Conley, Julia. 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians'. Truthout, 19 May

2024. https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/.

- Davies, Harry. 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data'. The Guardian, 10 August 2025. https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data.
- Davies, Harry, and Yuval Abraham. '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'. The Guardian, 6 August 2025. https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.
- Davies, Harry, and Yuval Abraham. 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'. The Guardian, 25 September 2025. https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israel Demanded Google and Amazon Use Secret "Wink" to Sidestep Legal Orders'. The Guardian, 29 October 2025. https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'. The Guardian (Jerusalem), 6 March 2025. https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.
- Davies, Harry, and Yuval Abraham. 'Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War'. The Guardian (Jerusalem), 23 January 2025. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.
- Davies, Harry, and Bethan McKernan. 'Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse'. The Guardian, 5 April 2024. https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse.
- De Luce, Dan. 'Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies'. NBC News, 20 September 2024. https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888.
- Decoster, Xavier Stephane, Ilhab Jebari, Anat Lewin, and Carlo Maria Rossotto. The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development. No. 104263. World Bank Group, 2016. http://documents.worldbank.org/curated/en/993031473856114803.
- Demopoulos, Alaina. 'Honk Honk! Can Noise Cameras Reduce "Potentially Fatal" Sound Pollution?' The Guardian (New York), 4 October 2023. https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras.
- Electronic Frontier Foundation. 'Gunshot Detection'. Street Level Surveillance, n.d. https://sls.eff.org/technologies/gunshot-detection.
- Euro-Med Human Rights Monitor. Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies. 13 November 2022. https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles,-stop-fully-cooperating-with-security-agencies.
- Fathallah, Sarah. 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine'. Public Humanities 2 (2026): e7. https://doi.org/10.1017/pub.2025.10113.
- Fathallah, Sarah. 'Artificial Intelligence and the Orchestration of Palestinian Life and Death'. Tech Policy Press, 12 August 2025. https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/.
- Fathallah, Sarah, and Nick Mitchell. 'Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life'. Disjunctions Magazine, January 2026. https://disjunctionsmag.com/articles/occupied-assets/.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 'From Data Mining to Knowledge Discovery in Databases'. AI Magazine, 15 March 1996.
- Flensburg, Sofie, and Signe Sophus Lai. 'Follow the Data! A Strategy for Tracing Infrastructural Power'. Media and Communication 11, no. 2 (2023). https://doi.org/10.17645/mac.v11i2.6464.
- Frenkel, Sheera, and Natan Odenheimer. 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns'. The New York Times, 25 April 2025. https://www.nytimes.com/202525/04//technology/israel-gaza-ai.html.

- Front Line Defenders. OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. Front Line Defenders, 2021. https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware.
- Goodfriend, Sophia. The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2021. https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf.
- Goodfriend, Sophia. 'When Palestinian Political Speech Is "Incitement"'. Jewish Currents, 15 September 2021. https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.
- Grim, Ryan, and Waqas Ahmed. 'The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal'. Drop Site, 23 January 2025. https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.
- Halabi, Usama. 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.43249780203845967/.
- Hassan, Zaha, and H. A. Hellyer. Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel. Oneworld Academic, 2024.
- Human Rights Watch. Questions and Answers: Israeli Military's Use of Digital Tools in Gaza. 10 September 2024. https://www.hrw.org/news/202410/09//questions-and-answers-israeli-militarys-use-digital-tools-gaza.
- Human Rights Watch. Spyware Used to Hack Palestinian Rights Defenders. 8 November 2021. https://www.hrw.org/news/202108/11//spyware-used-hack-palestinian-rights-defenders.
- IMEU. Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement. Institute for Middle East Understanding, 2021.
- Investigate. 'Amazon.Com Inc.' The American Friends Service Committee, 7 August 2024. https://investigate.info/company/amazon.
- Investigate. 'Microsoft Corp.' The American Friends Service Committee, 29 January 2025. https://investigate.info/company/microsoft.
- James, Robin. 'Acousmatic Surveillance and Big Data'. Sounding Out!, 20 October 2014. https://soundstudiesblog.com/201420/10//the-acousmatic-era-of-surveillance/.
- Jamil, Yassin. '"Tafāṣīl Muḏhila ʿan Ṭuruq Wa ʾasālīb al-Murāqaba as-Sirrya al-Isrāʾīlya Lil-Hawātif al-Jawwāla Lil-Muqāwama al-Filsṭīnya Wal-Lubnānya" تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel's Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]'. Rai Alyoum, 21 June 2016. https://www.raialyoum.com/تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة/.
- Kelley, Hannah. 'Dual-Use Technology and U.S. Export Controls'. CNAS Technology Policy Lab, 15 June 2023. https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.
- Leix Palumbo, Daniel, and Robert Prey. 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice'. Big Data & Society 11, no. 4 (2024): 20539517241297889. https://doi.org/10.11772053951724129788 9/.
- Leufer, Daniel. 'Sonic Surveillance: Why You Don't Want AI Snooping on You'. Access Now, 23 September 2025. https://www.accessnow.org/ai-snooping/.
- Ludwig, Mike. 'Microsoft Faces Reckoning for Assisting Israel's Genocide in Gaza'. Truthout, 3 December 2025. https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/.
- Mahmoud, Khalid Walid. 'Voiceprint: From a Verification Tool to a Tracking Technology'. The Peninsula, 19 January 2025. https://thepeninsulaqatar.com/opinion/192025/01//voiceprint-from-a-verification-tool-to-a-tracking-technology.
- Mann, Yuval, and Korin Elbaz-Alush. 'Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says'. YNet, 27 June 2023. https://www.ynetnews.com/business/article/hjmohud002.
- Marciano, Avi. 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity'. Surveillance & Society 19, no. 1 (2021): 85–88. https://doi.org/10.24908/ss.v19i1.14543.

- Masarwa, Lubna. 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'. Middle East Eye (Jerusalem), 15 November 2021. https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.
- McClain, Jade. 'Alexa, Am I Happy? How AI Emotion Recognition Falls Short'. New York University, 18 December 2023. https://www.nyu.edu/about/news-publications/news/2023/december/alexa--am-i-happy--how-ai-emotion-recognition-falls-short.html.
- Mhawish, Mohammed R. 'Watched, Tracked, and Targeted'. New York Magazine, 3 December 2025. https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html.
- Microsoft. 'Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza'. Microsoft On the Issues, 15 August 2025. https://blogs.microsoft.com/on-the-issues/202515/05//statement-technology-israel-gaza/.
- Microsoft. Microsoft to Launch New Cloud Data Center Region in Israel. 22 January 2020. https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/.
- Microsoft. What Is the Speech Service? 5 November 2025. https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview.
- Mitnick, Josh. 'Here's How the Israeli Army Is Embracing Digital Transformation'. CIO, 8 February 2020.
- Mossad, Marco. 'Are Global Tech Giants Facilitating Israel's War on Gaza?' Al Majalla, 31 May 2024. https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E299%80%s-war-gaza.
- Mossad, Marco. 'Voiceprint Technology: A Commercial Hit with Military Utility'. Al Majalla, 7 February 2024. https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility.
- Mullett, Layne. 'Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide'. American Friends Service Committee, 23 July 2025. https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide.
- Niang, Sophie Marie. 'In Defence of What's There: Notes on Scavenging as Methodology'. Feminist Review 136, no. 1 (2024): 52–66. https://doi.org/10.1177/01417891231222606/.
- Nissenbaum, Helen. 'Accountability in a Computerized Society'. Science and Engineering Ethics 2, no. 1 (1996): 25–42. https://doi.org/10.1007/BF02639315.
- No Azure For Apartheid. The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200. 25 September 2025. https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b.
- O'Brien, Danny, and Jillian C. York. 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?' Electronic Frontier Foundation, 11 November 2015. https://www.eff.org/deeplinks/201511//palestine-3g.
- O'Carroll, Lisa. 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'. The Guardian, 4 December 2025. https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf.
- Oslo Accords. Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II). 1995. https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.
- Palestine Today. '"Kayfa tatanaṣat ālmuḫābarāt āl'isrāīlya ʿalā jawwālik āšaḫsy!?" كيف تتنصت المخابرات الإسرائيلية على جوالك الشخصي! [How does Israeli intelligence eavesdrop on your personal mobile phone?!]'. Palestine Today, 30 December 2013. https://paltodaytv.com/post/466/كيف-تتنصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي.
- Privacy International. The Global Surveillance Industry. 2016. https://privacyinternational.org/sites/default/files/201712-/global_surveillance_0.pdf.
- Reuters. 'Israeli Defense Ministry Launches COVID-19 Voice-Test Study'. Reuters (Jerusalem), 24 March 2020. https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/.
- Reuters. 'Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to $3 Billion, Report Says'. 30 December 2025. https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-202530-12-/.

- Sada Social. Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military. 18 May 2024. https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdmy-oatsab-l-algysh-alsrayly.
- Sa'di, Ahmad H. Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority. Manchester International Relations. Manchester University Press, 2016.
- Salah, Hana. '"Albaṣma as-Ṣaūtya" Adāt Isrā'īl Litanfīḏ Syāsat "Attaṣafya al-Jasadya" "البصمة الصوتية" أداة إسرائيل لتنفيذ سياسة "التصفية الجسدية" ["Voiceprints": Israel's Tool for Implementing "Elimination"]'. Al-Monitor, 4 February 2014. https://www.al-monitor.com/ar/contents/articles/originals/201402//gaza-israel-islamic-jihad-hamas-mobile-war.html.
- Salah, Mohamad Ateyyah, Mohamad Shalodi, and Mahmoud Skafi. 'Voiceprint Authentication System'. Palestine Polytechnic University, 2021. https://scholar.ppu.edu/bitstream/handle/1234567897547//Voiceprint-Authentication-System.pdf.
- Shalhoub-Kevorkian, Nadera. Security Theology, Surveillance and the Politics of Fear. 1st edn. Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781316159927.
- Shalhoub-Kevorkian, Nadera, and Abeer Otman. 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023. Secrecy as Colonial Violence.
- Siddiqui, Usaid. '"Chilling Effect": Israel's Ongoing Surveillance of Palestinians'. Al Jazeera, 8 May 2023. https://www.aljazeera.com/news/20237/5//chilling-effect-israels-ongoing-surveillance-of-palestinians.
- Smalley, Suzanne. 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker'. The Record, 20 November 2025. https://therecord.media/nso-seeks-to-overturn-whatsapp-case.
- Smith, Brad. 'Update on Ongoing Microsoft Review'. Microsoft On the Issues, 25 September 2025. https://blogs.microsoft.com/on-the-issues/202525/09//update-on-ongoing-microsoft-review/.
- Stanley, Jay. 'On the Creation of Giant Voiceprint Databases'. ACLU, 16 October 2014. https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases.
- Swinhoe, Dan. AWS Launches Israeli Cloud Region in Tel Aviv. 2 August 2023.
- Tawil-Souri, Helga. 'Digital Occupation: Gaza's High-Tech Enclosure'. Journal of Palestine Studies 41, no. 2 (2012): 27–43. https://doi.org/10.1525/jps.2012.XLI.2.27.
- Tawil-Souri, Helga. 'Hacking Palestine: A Digital Occupation'. Al Jazeera, 9 November 2011. https://www.aljazeera.com/opinions/20119/11//hacking-palestine-a-digital-occupation.
- Tawil-Souri, Helga. 'Israel's Telecommunications Lines and Digital Surveillance Routes'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023.
- Tawil-Souri, Helga. 'Surveillance Sublime: The Security State in Jerusalem'. Jerusalem Quarterly, no. 68 (December 2016): 56–65. https://doi.org/10.70190/jq.I68.p56.
- The Office of the High Commissioner for Human Rights. 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. A/HRC/592025 .23/. https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur.
- The Palestine Chronicle. 'Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media'. 18 February 2026. https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/.
- The Times of Israel. 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'. The Times of Israel, 26 April 2025. https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.
- Zureik, Elia. 'Colonialism, Surveillance, and Population Control'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.43249780203845967/.

- Zureik, Elia, and David Lyon. 'Coronavirus Surveillance and Minority Groups in Israel/Palestine'. The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.
- Zureik, Elia T. Israel's Colonial Project in Palestine: Brutal Pursuit. Routledge Studies on the Arab-Israeli Conflict 20. Routledge, 2016

سرديات مدفوعة الأجر:

التضليل الإعلامي وتأثير الدولة عبر إعلانات جوجل

ميلودي سيباهبور- فارد

ميلودي مرشحة دكتوراه في علم البيانات بجامعة ليمريك. وبخلفية تجمع علم النفس والعلوم الاجتماعية الحاسوبية، تبحث ملودي الهوية والخطاب والمعلومات المضللة عبر الإنترنت. واستكشفت موضوعات تمتد من تضليل اللقاحات إلى النشاط الشبكي متعدد اللغات.

يحلل مشروع ميلودي البحثي الإعلانات الرقمية الموجّهة للجمهور الأوروبي، وبخاصة الحملات الصادرة عن هيئة الإعلانات الحكومية الإسرائيلية. وتدرس كيف تتطور هذه الإعلانات وتنشر المعلومات المضللة وتؤثر في الرأي العام، مع تقييم مدى التزامها بسياسات الشركات والاتحاد الأوروبي وآثارها الواقعية.

إيجاز

يُعاين هذا المقال استخدام الدعاية وإعلانات جوجل كأداة في التأثير المعلوماتي المرتبط بالدول، ويُركز على مجموعة بيانات إعلانية منسوبة إلى الحكومة الإسرائيلية على مدار سبعة أشهر. تُشخص الدراسة بالاستناد إلى مجموعة بيانات أصلية جُمعت من مركز شفافية إعلانات جوجل، مجموعات ثيمات (موضوعات) متكررة، كحملات تستهدف مؤسسات قانونية دولية، التقارير الإنسانية عن غزة، والتي تتزامن مع فترات تصاعد الاهتمام السياسي والإعلامي. يجمع التحليل بين المنهجين الكمي والنوعي.

أولًا، يقوم المقال برسم خريطة للديناميكيات الزمنية والاستهداف الجغرافي والتوزيع الموضوعي للإعلانات، مُظهرًا أن نشاط الحملات مُنظم في دفعات قصيرة وعالية الكثافة تتماشى مع أحداث محددة.

ثانيًا، يقوم المقال بتقدير مدى الانكشاف على الاعلانات باستخدام نطاقات الانطباع والظهور، ويُعيد بناء أنماط الظهور اليومية، كاشفًا كيف يهيمن عدد قليل من المواضيع على وصول الجمهور.

ثالثًا، تُجري الدراسة تحليلًا نوعيًا لإعلانٍ ما لدراسة كيفية بناء السرديات، مع التركيز بشكل خاص على استراتيجيات تجريد المعلومات من سياقها، وتأطيرها، ونزع الشرعية عن الجهات الفاعلة الدولية. تُشير النتائج إلى عمل إعلانات جوجل كبنية تحتية عالية التأثير للتواصل والإعلام الاستراتيجي، مما يُمكّن الهيئات والجهات الحكومية من إدراج سرديات مُفضّلة عندما يبحث المستخدمون بشكل نشط عن معلومات حول قضايا وشؤون محط النزاع.

رُغم عدم تصنيف هذه الإعلانات كذات طابع سياسيّ بموجب سياسات المنصّة، إلا أنها غالبًا ما تتناول مواضيع حساسة سياسيًا، وقد تُساهم في نشر المعلومات المُضللة على نطاق واسع. تختتم المقالة بمناقشة الآثار المترتبة على دراسة وأبحاث المعلومات المُضللة، وحوكمة المنصات، وتنظيم الإعلانات المعنية بالقضايا والخلافات في البيئات الرقمية.

1. توطئة

أيام قليلة بعد السابع من تشرين الأول، زعمت حسابات إسرائيلية أن مقاتلي حماس. «قطعوا رؤوس 40 طفلًا رضيعًا» [41، 40]. وانتشرت هذه الرواية على نطاق واسع في الإعلام الغربي، لدرجة أن الرئيس الأمريكي في حينه، جو بايدن، ادعى أنه شاهد صور الأطفال الرُضّع [10]. يعكس هذا الاتهام إحدى أكثر قصص المعلومات المُضللة صدمة وتأثيرًا التي ظهرت من تقارير إعلامية حول الحدث. رغم أنه سُرعان ما قام صحافيون ومستقصو الحقائق بتفنيدها، لعدم عثورهم على أي دليل يدعم هذه المزاعم، واصلت القصة بالانتشار وصياغة التصوّرات عن الصراع [10]. الاستمرار بتداول هذه المعلومات المُضللة هو خير مثال للدور الذي تلعبه السرديات المشحونة عاطفيًا، ما إن تُطلق إلى الفضاء المعلوماتي، في

تطوير مناعة مُعتبرة بمواجهة التصحيح القائم على الحقائق، وذلك بفضل قدرتها على مخاطبة المعتقدات والتحيّزات [45]. تهدف هذه المشاهد والصور المشحونة عاطفيًا للوحشيّة الشديدة ضد الأطفال الأبرياء إلى منع تطوير نقاش موضوعي عقلاني وتشجيع الدعم الجماهيري العام للتدخل العسكري.

لم تكن سردية الـ»40 طفلًا رضيعًا مقطوعي الرأس» حادثة معزولة، بل جزء من نمط أوسع من التضليل المعلوماتي[1] الذي ظهر وذي علاقة بعد السابع من أكتوبر السابع من أكتوبر. كما تم تداول العديد من الادعاءات والمزاعم الأخرى في الخطاب الإعلامي رغم افتقاده لأي تأكيد موثوق: إستخدام حماس للدروع البشرية كسياسية مُمنهجة، شيوع اقتراف مقاتلي حماس للعنف الجنسي وعمليات الاغتصاب، انخراط عملاء الاستخبارات من حماس في صفوف وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين (أونروا)، وغيرها المزيد. تعكس هذه الأمثلة نمطًا من تضخيم المزاعم غير المؤكدة وذات السياق المُشوّه بشدّة عبر قنوات رسمية ووسائل الإعلام، مما يخلق ما يسميه الباحثون «أثر غرفة الصدى» (أو أثر الغرفة الصدوية)[2] حيث يغلب التكرار، الحدّة العاطفية، والتحيّز التأكيدي[3] التأكيد الوقائعي والحقائق [16، 45].

عدا عن خلق مجازات وصور سلبية عن الفلسطينيين، تبني حملات التضليل الإعلامي الإسرائيلية بشكل استراتيجي سرديات توّفر تبريرات أخلاقية للحرب والإبادة الجماعية. وتتعدى قوّة هذه السرديات الكاذبة تجريد المجموعة السكانية المُستهدفة من انسانيتها، لدرجة خلق إلحاح وضرورة أخلاقية في القيام بعملية عسكرية، مما يصوّر الصراع على أنه بين حضارة مُتحضّرة والبربر الهمجيين.

يُتيح النظام البيئي الرقمي في عصرنا الراهن رواجًا فوريًا وواسع الانتشار دوليًا للسرديات الكاذبة. يُتيح الانترنت للمعلومات المُضللة تخطي الحرس التقليدي والانتشار بشكل جرثومي عبر منصات التواصل الاجتماعي، مُحركات البحث، وتطبيقات المُراسلة. خلق العصر التكنولوجي الحالي ظروفًا غير مسبوقة تُتيح التلاعب برأي الجمهور مُباشرة وفورًا، ووصول السرديات الكاذبة عن الصراعات للملايين من البشر في غضون ساعات وتشكيل التصوّرات العالمية حتى قبل بدء جهود التحقق من الحقائق [62، 71].

بحثت العديد من الدراسات التضليل المعلوماتي عبر الانترنت [48، 15، 9، 67]، عبر مجموعات من الأفراد ومجموعات مُنظمة ذات علاقة بالتأثير الأجنبي [47، 43، 51]. ركّزت الغالبية العُظمى من الأبحاث في مضمار التأثير الأجنبي على التأثير الروسي على المجتمعات الغربية، واستفاضت في تفصيل الحملات المُتطوّرة والمُعقدة التي تعمد إلى توظيف شبكات البوتا، مصانع متصيّدي الانترنت (Troll factories)، والتلاعب المُنسّق عبر وسائل التواصل للتأثير على الانتخابات، تقويض المؤسسات الديمقراطية، وصقل وبناء السردية الجيو-سياسية [11، 36، 49، 30، 46].

1 المعلومات الكاذبة التي يتم مشاركتها عن قصد لإحداث ضرر [73]

2 إنشاء مجموعات قائمة على الرأي الواحد مع انكشاف نادر لوجهات نظر متنوّعة عبر وسائل التواصل الاجتماعي، مما يُعزز المُعتقدات المُشتركة [16]

3 ميل الأفراد المنهجيّ للبحث، تحليل، تذكر، وإعطاء قيمة أكبر لمعلومات تؤكد معتقداتهم، توقعاتهم، ونظرياتهم القائمة [53]

إلا أن التضليل الإعلامي الصادر عن جهات دولية فاعلية أخرى كاسرائيل، لا يزال غير مدروسٍ بشكلٍ كافٍ. على سبيل المثال، وثّق بحث أجراه فريق East StratCom Task Force التابع للاتحاد الأوروبي في إطار مشروع EUvsDisinfo بشكل منهجيّ الاستراتيجيات، السرديات، والآثار عابرة الحدود لتضليل المعلومات المُدعوم من الدولة الروسية على عدد من الدول والسياقات السياسية [27]. في المقابل، ورغم عدد لا يُحصى من حالات التضليل المعلوماتي الإسرائيلي المُوّثقة، لا تزال التحقيقات والأبحاث المنهجية الأكاديمية لحملات التضليل المعلوماتي المدعومة من الدولة الاسرائيلية؛ غائبة بالعموم من المشهد البحثي. هذه الفجوة البحثية تتواصل رغم وجود أدلة واضحة على توظيف السلطات الاسرائيلية لعمليات استراتيجية معلوماتية مُعقدة، وعلى كونها قادرة على الوصول للإعلام الغربي والمنصات التكنولوجية، وعلى بذلها جهودًا مُنظمة ومنهجية لأجل صياغة وتشكيل التصوّرات الدوليّة عن الصراع الإسرائيلي – الفلسطيني [29، 42، 4، 2، 3، 68].

تناقش هذه الورقة البحثية عدة أسئلة بحثية نقدية:

كيف تستخدم الحكومة الاسرائيلية منصة جوجل للإعلانات كأداة للتأثير المعلوماتي؟
ما هي السمات الزمانية، الثيماتية (الموضوعاتية)، والجغرافية لهذه الحملات الإعلانية؟
كيف تُبنى هذه السرديات في إطار الإعلانات، وإلى أي مدى تعتمد على أشكال التصوير المُضللة أو الخارجة عن السياق؟

للإجابة على هذه الأسئلة، تنتهج دراستنا نهج الأساليب والمنهجيات المتنوّعة، التي تدمج بين التحليل الكميّ لبيانات إعلانات جوجل Google ad والتحليل النوعيّ للسرديات المُدمجة في هذه الإعلانات. عبر المنهجيات الكميّة، نقوم بتحليل مُحتوى الإعلان، استراتيجيات الاستهداف، أنماط النشر والتوزيع، ووصول حملات الحكومة الإسرائيلية المعلوماتية المُضللة على شتى منصات جوجل. تدعيمًا لهذا التحليل الكميّ، تشمل الورقة البحثية مُعاينة نوعيّة لإعلان بهدف تحليل كيفية صياغة وبناء السرديات وإنتاج المعلومات المُضللة عبر تقنيات كالاقتباس الانتقائي، الإخراج عن السياق، والتأطير المُضلل. تسمح لنا هذه المنهجية المُزدوجة بتوثيق آليات المعلومات المُضللة الرقمية والكشف عن الوظائف الأيديولوجية الفكرية التي تحملها في محاولة تصوير الهُويّات الفلسطينية كتهديد يجب القضاء عليه عوضًا عن كونهم بشر لهم حقوق مُستحقة.

يتناول القسم التالي من الخلفية، بثلاثة أجزاء، آليات التضليل الإسرائيلي وتضخيمه عبر المنصات الرقمية. أولًا، نضع الأساس لاطار نظري شامل لفهم التضليل الإعلامي، تحليل قواعده المعرفية، والتحديات المستدامة في التقليل من أثره. ثانيًا، نعاين الـ «هسبارا» الإسرائيلية، بمعنى نظام الدعاية والدبلوماسية العامة والاتصالات الاستراتيجية المموّل من دولة إسرائيل، الهادف إلى صياغة وصقل التصوّرات الدولية حول الأفعال والسياسات الاسرائيلية، بالذات تلك التي تُعنى بفلسطين. سنستقصي مسار تطوّرها التاريخي، أهدافها، منهجياتها في صياغة وبنيان السرديات العالمية المعنية باسرائيل وفلسطين. وأخيرًا، سنحقق في دور جوجل كمنصة تنتفع وتستفيد من المعلومات المُضللة وتضخيمها. مُجتمعّة، توّفر هذه الأجزاء الثلاثة تحليلًا مُتعدد الأبعاد يتناول كيفية صناعة وإنتاج المعلومات

المُضللة، نشرها بشكل استراتيجي، وتضخيمها من قبل الحكومة الاسرائيلية من خلال المنصات الرقمية في سياق ارتكاب إسرائيل للإبادة الجماعية ضد الشعب الفلسطيني [7، 70]، مما يقدّم رؤى معمقة حول التفاعل المُعقّد بين سلطة الدولة والمنصات الرقمية وتلاعب الحكومة الإسرائيلية بالمعلومات، كونها جهة فاعلة لم تحظ بدراسات وازنة أو كافية.

2. الخلفية

يقدّم هذا الفصل السياق الإصطلاحيّ والمعرفيّ والتجريبيّ للدراسة. ويستعرض أولًا تعريف وآليات التضليل الإعلامي، ثم يُحلّل الأدلة المتوفرة حول التأثير المعلوماتي المرتبط بالدولة الإسرائيلية، ويناقش أخيرًا دور جوجل كبنية تحتية للظهور والتأثير السياسيّ القائم على الإعلانات.

2.1 التضليل الإعلامي: تعريف وآليات

يستعرض هذا القسم الأسس المفاهيمية والاصطلاحية للتضليل الإعلامي. ويوّضح بادئ ذي بدء التعريفات الأساسية المُستخدمة بالأدبيات؛ ومن ثم يعاين الآليات النفسية السيكولوجية والإعلامية التي تشرح جدواه؛ وأخيرًا، يموضع النقاش ضمن إطار الأدبيات الأوسع، والذي يُركّز بشكل أساسي على تأثير الدولة الروسية.

2.1.1 تعريف

عند إجراء بحث عن «الأخبار الكاذبة» والتضليل المعلوماتيّ، من المهم أن نتنبّه إلى أن المحتوى الكاذب ليس عبارة عن ظاهرة واحدة ووحيدة، بل مجموعة من المُمارسات المرتبطة ذات حوافز، سلاسل توليد، وأثار مؤذية مختلفة ومتنوعة. بموجب الإطار العام الشائع، يُميّز واردل وديراخشان [73] بين المعلومات المُضللة misinformation (أي، معلومات كاذبة أو خاطئة تتم مشاركتها عن غير قصد احداث الضرر) وبين التضليل الإعلامي disinformation (أي معلومات كاذبة أو خاطئة يُقصد انتاجها ومشاركتها بهدف إحداث الضرر). هذا التمييز مُفيد في الجانب التحليلي، إذ أنه يُبرز دور القصد والنية بإحداث الضرر والايذاء، آخذًا بالحسبان شتى الجهات الفاعلة المتورطة في إنتاج، صناعة، وتوزيع ونشر المعلومات [73].

رغم ذلك، لا تُطبق هذه الفئات بشكل متواصل في الأدبيات: بعض الدراسات تستخدم «المعلومات المُضللة» كاصطلاح عام يشمل التلاعب السياسي المقصود [45، 23].

علاوة على ذلك، غالبًا ما تُعرّف دراسات مؤثرة حول «الأخبار الكاذبة» (fake news) الظاهرة كمعلومات مُلفقة تُحاكي محتوى وسائل الإعلام الإخبارية شكلًا وتفتقد للصيرورة أو النية التنظيمية، في حين تُشدد على الشكل والمُحاكاة الاستراتيجية عوضًا عن عدم الدقة الوقائعية [44].

توّظف هذه الورقة البحثية التضليل الإعلامي كمفهوم رئيسي لسببين. أولًا، تُعنى الحالات الإمبيرية التجريبية التي تشكل السبب المُحفز لهذه الدراسة، بتوظيف الادعاءات الكاذبة أو المُضللة في بيئة نزاعية استراتيجيًا في ما يُرجح أن الهدف هو

صياغة أو تشكيل التصوّرات، أو إضفاء الشرعية على العنف، أو نزع الشرعية عن جماعة خارجية. تلائم هذه الأهداف وصف التواصل الاعلامي السياسي المقصود أكثر من احتمال لأن تكون محض صدفة أو خطأ عشوائي، وهذا التمييز بين الأمرين ضروري إذا ما كنا نسعى لفهم الأسباب الكامنة في نشر المعلومات الخاطئة [73]. ثانيًا، كون المشروع يُركّز على حملات مرتبطة بالدول والبُنى التحتية المأجورة للنشر والتوزيع (بما معناه، أنظمة الدعاية والاعلان)، يصبّ الوكيل ومحفزّاته في صُلب التحليل، وهو بالضبط ما يسعى مفهوم التضليل الإعلامي لتجسيده [73، 74].

2.1.2 آليات المشاعر والتكرار

يكون التضليل الإعلامي أكثر إقناعًا عندما يُثير العاطفة، ويجذب البصر، ويسهل تكراره، ويكون مُضمنًا في قصة متماسكة، وذي سردية قوية [73، 17، 38، 58]. تُظهر الأبحاث في علم النفس أن الناس أكثر ميلًا لمشاركة المعلومات التي تُثير مشاعر قوية (مثل الاشمئزاز والخوف والغضب)، في غالب الأحيان غير كارثين بصحتها من عدمها]12، 38[. ولذلك، يمكن أن تكون سرديات الفظائع - وخاصة تلك التي تشمل فظائع ضد الأطفال - أمثلة قوية على هذا المنطق، كونها تجعل الفرد يستشيط غضبًا على المستوى الأخلاقي ولها فعل فوري، كما تُقدم تصوّرًا مُتخيّلًا حيًا قد يدوم حتى بعد أي تصحيحات لاحقة]20[. كما أن لها ثلاثة أهداف رئيسية [20]: 1) شيطنة العدو، 2) حشد الدعم المحلي والدولي، 3) تبرير التصعيد أو التدخل. وظيفتها ليست تقديم تفاصيل فعلية، بل خلق مخطط أخلاقي يكون فيه أحد الجانبين إنسانيًا والآخر وحشيًا [20]. يزيد التكرار من المصداقية المُتصوّرة. وقد وجدت دراسات كلاسيكية تناولت النميمة والشائعات أن تكرار الشائعات من شأنه أن يتنبأ بالايمان بصحة الشائعات زمن الحرب [5]. وتُظهر أبحاث لاحقة أن العبارات المُكررة تبدو أكثر ألفة، وبالتالي أكثر «صحة»، حتى عندما يكون التكرار سطحيًا أو عرضيًا، وهي ظاهرة تُعرف بأثر وهم الحقيقة [37]. وفي السياقات السياسية، يُشكل هذا خطرًا بنيويًا: فحتى التحقق من الحقائق بحسن نية قد يُساهم عن دون قصد في نشر الادعاء الكاذب من خلال زيادة ألفته [44، 23].

الانحياز المعرفيّ

يحمل التضليل الإعلامي فاعليّة خاصة حينما يؤكد معتقدات قائمة. التحيّز التأكيدي هو الميل للبحث، تحليل، وتذكر معلومات بطرف تؤكد على المعتقدات القائمة مُسبقًا [53]. تُبيّن أبحاث ودراسات سابقة في الإعلام السياسي أن الجماهير تُفضّل معلومات متسّقة المنهج (الانكشاف النتقائي) وتقيّم ادعاءات متناغمة مع آرائها كمُقنعة بدرجة أعلى من الادعاءات غير المتناغمة مع آرائها [63]. كما يتقبل الناس معلومات كونها مرغوبة سيكولوجيًا – بكلمات أخرى، الانحياز للمقبول اجتماعيًا [25، 24، 44]. تحمل هذه الآليات أهمية كُبرى بما يتعلق بالتضليل الإعلامي، إذ أن الصور النمطية والتصوّرات العنصرية يمكن أن تلعب دور الأفكار المسبقة وتجعل الادعاءات المتطرفة تبدو معقولة [57]. حينما تُلائم المعلومات الجديدة الوافدة فرضيات قائمة عن مجموعة الهدف، تتم مُعالجتها بسلاسة أكبر ومن الراجح ألا تُثير التشكيك؛ أما حينما تناقض مُعتقدات سابقة فمن الأرجح أن يتفحّصها الناس بإمعان أكبر أو حتى رفضها [45، 23]. بعبارات أخرى، لا يعمل التضليل الإعلامي على الاقناع من فراغ؛ بل إنه ينجح في الغالب من خلال مخاطبة وتفعيل ما تفترضه الجماهير أصلًا.

المثابرة وفشل التصحيحات

رغم عرض التصحيحات مرارًا وتكرارًا كالإصلاح الرئيسي للتضليل الإعلامي، تُبين الدراسات والأبحاث بشكل مستمر أن أثرها محدود. في العديد من الحالات، تبقى وتتواصل آثار التضليل الإعلامي حتى بعد تلقي التصحيحات، فهمها، وتذكرها، مما يكشف عن انعدام التماثل المنهجي القائم بين قوة التضليل الإعلامي على صياغة وتشكيل التصوّرات الذهنية المُتخيّلة وقدرة المعلومات الصحيحة الضعيفة إلى حدٍ كبير على تصحيحها. الموجز التوليفي من ليفاندوفسكي، ايكر، وكوك]45[يراجع الأدلة والبيّنات على أثر التأثير المستمر: حتى عندما يحصل الناس على ارتداد أو تراجع ويتذكرونه، يواصلون الاعتماد على المعلومات المُضللة في منطقهم وذاكرتهم. ويؤكد تحليل تجميعي أن المعلومات المُضللة تميل للاحتفاظ بالأثر المُعتبر حتى بعد التصحيح بشكل قاطع للعديد من السياقات]72[. وجد التحليل التجميعي أن التصحيحات تكون مؤثرة بدرجة أقل بكثير حينما تُنسب المعلومات المُضللة إلى مصدر موثوق، حينما تُكرر مرات عدّة قبل التصحيح، أو حينما يكون هناك تأخيرًا زمنيًا بين الانكشاف للمعلومات المُضللة وللارتداد اللاحق أو التراجع عنها في وقت لاحق. بالمقابل، فإن التصحيحات تميل لأن تكون ناجحة بدرجة أكبر حينما تكون متماسكة، تتماشى مع الآراء والتصوّرات العامة القائمة لدى الجمهور، وتكون صادرة عن المصدر ذاته الذي نقل المعلومات المُضللة. تُشير الدراسات المعاصرة إلى أن مقاومة التصحيح تتشكل بفعل عوامل معرفية (التفكير الحدسي، ضعف الذاكرة، والألفة) وعوامل اجتماعية عاطفية (الهُويّة، الانتماء الجماعي، مؤشرات المصدر، نظام المعتقدات أو التصوّرات العامة، والعواطف) [23]. أحد أسباب فشل التصحيحات هو أن المعلومات المُضللة غالبًا ما تُقدم قصة سببية بسيطة. قد تُحدث الارتدادات أو التراجعات فجوة تفسيرية ما لم تُقترن بسردية بديلة تُعيد التماسك، وهو نهج أثبت فعاليته في تحسين فعالية التصحيح [45]. سبب آخر هو أن الناس قد ينسون السياق الذي صادفوا فيه الادعاء مع احتفاظهم بالانطباع العاطفي والارتباط، خاصةً في ظل كثرة التكرار [44، 37].

2.1.3 تركيز الأدبيات على روسيا

ركزت الجهود المؤسسية والأكاديمية في مجال التضليل الإعلامي بشكل غير متناسب على تأثير الدولة الروسية، لا سيما بعد انتخابات الولايات المتحدة لعام 2016 والمخاوف الأوروبية اللاحقة بشأن الحرب المعلوماتية]11، 36، 49، 30، 46[. بحث مؤسساتي مركزي مُعتمد هو بحث فريق East StratCom Task Force التابع للاتحاد الأوروبي ومشروعه EUvsDisinfo الذي يصنّف ويُحلل سرديات التضليل الإعلامي المؤيدة لروسيا وتداولها عبر الدول]27[. هذا التركيز ساهم في تعريف التضليل الإعلامي في السواد الأعظم من الخطاب السياسي والعام: دولة أجنبية فاعلة توّظف رسائل مُتسّقة بهدف زعزعة والإضرار بالتماسك السياسي، الثقة، والنظام الديمقراطي]54، 28[. يُقدّم تقرير مؤسسة راند RAND المؤثر حول نموذج «سيل الأكاذيب» دروسًا مُلخّصة حول الدعاية الروسية الحديثة، ويُشير بالأساس إلى: (1) النشر واسع النطاق عبر قنوات متعددة، (2) التكرار السريع والمستمر، (3) عدم الالتزام بالواقع الموضوعي، و(4) الرسائل المتضاربة المصممة لإرباك الجمهور وإغراقه بأفكار مُربكة]56[. بدلاً من الإقناع من خلال الحجج الدقيقة، يهدف هذا النهج إلى صياغة وتشكيل البيئة المعلوماتية من خلال الإشباع، السرعة، والتكرار، بغية إنتاج الألفة وبالتالي أن يزيد صعوبة التصحيح [56، 37، 45].

مسار كبير لتوزيع ونشر التضليل الإعلامي يمرّ عبر الدعاية المحوسبة أو الكتائب السيبرانية وكيف تقوم الدول بتنظيم وتوظيف الاحتيال والتلاعب بواسطة التواصل الاجتماعي كمُمارسة استراتيجية. تُظهر مخزونات معهد أوكسفورد للانترنت العالمية أن الاحتيال المُنظم عبر التواصل الاجتماعي شائع الانتشار ويُصبح مُشخصنًا بدرجات أكبر عبر العديد من الدول، وليس روسيا فحسب [13، 14].

كما تعكس تعريفات المنصات هذا التوّجه: فقد عرّف فريق «فيسبوك» للأمن «العمليات المعلوماتية» كأفعال واجراءات متسّقة من قبل الحكومات أو الفاعلين المُنظمين لتشويه الإحساس والعاطفة السياسية، غالبًا باستخدام حسابات وهمية والتضخيم المُتسّق [74].

تدعم هذه المجموعات من الأعمال مُجتمعةً ثلاثة استنتاجات رئيسية: 1) التضليل الإعلامي غالبًا ما يكون مُنظمًا واستراتيجيًا وليس عفويًا؛ 2) تلعب البُنى التحتية الرقمية وقدرات المنصة الوظيفية دورًا مركزيًا في مدى جدواها ونجاعتها؛ 3) التكرار، التضخيم، والسرديات المتناغمة مع الهُويّة تجعل من التضليل الإعلامي مقاوِمًا للتصحيح خلافًا للعادة [56، 23].

2.2 التضليل الإعلامي من الدولة الإسرائيلية

يعاين هذا القسم التنظيم وخصائص عمليات التأثير والنفوذ المرتبطة بالدولة الاسرائيلية. يستعرض بداية الأدلة المتوّفرة المعنية بنطاق هذه العمليات، ومن ثم يناقش مفهوم الـ»هسبارا» (الدعاية الاسرائيلية) كإطار عمل لفهم ممارسات اسرائيل الاعلامية الاستراتيجية.

2.2.1 نطاق العمليات

في حين أنه لا تُؤخذ إسرائيل بالعادة كحالة بحثية في الأدبيات، تُشير تيارات مُتعددة من الأدلة إلى وجود نشاط للتأثير مرتبط باسرائيل ويُغطي الدولة، الجهات الفاعلة الخاصة، والمواطنين. تُصنف مخزونات «الكتائب السايبرانية» التابعة لمعهد أوكسفورد للانترنت OII دولة اسرائيل كلاعب ذي كفاءة عالية، دائم، وذي تنسيق مركزي، في الاحتيال والتلاعب المُنظم عبر وسائل التواصل الاجتماعي، إلى جانب دول أخرى أمثال روسيا، الصين، المملكة العربية السعودية، والولايات المتحدة الأمريكية]14[. مما يُميّز فرق الكتائب السايبرانية عالية الكفاءة كونها تتدخل في العمليات الخارجية والمحلية أيضًا، اضافة لاستخدام المُشغّلين البشريين المتسقين والحسابات المؤتمتة، وفي بعض الحالات أيضًا، تخصيص موارد للإعلام المدعوم من الدولة وجهود الدعاية السرية [14].

يُشير مخزون معهد أوكسفورد للانترنت 2019 إلى أدلة إضافية على التدريب الرسمي ويقدّر حجم الفريق العامل بما يوازي نحو 400 فرد، إلى جانب عقود متعددة تُقدّر قيمتها بنحو 778 ألف دولار و 100 مليون دولار مرتبطة بالكتائب السايبرانية الإسرائيلية [3]. تُغطي هذه الأنشطة عدداً من المنصات، بينها فيسبوك، تويتر، وانستغرام؛ وتوظّف سلسلة من الاستراتيجيات كالرسائل الداعمة للحكومة، مهاجمة الخصوم السياسيين، قمع السرديات المقاومة، وسائط مرئية مُضللة أو متلاعب بها، استهداف مدفوع بالبيانات، التصيّد على الانترنت (Trolling)، والتضخيم المُنسّق [13، 14]. يوّثق معهد أوكسفورد للانترنت بالتحديد التنسيق الرسمي بين

الوكالات الحكومية والوزارات ومجموعات المجتمع المدني أو مجموعات المواطنين في باقة من الدول؛ وفي الحالات المعنية باسرائيل، يُذكر حشد مجموعات الشباب أو الطلبة الجامعيين، أو توظيفهم من قبل هيئات حكومية للمشاركة في الدعاية المُحوسبة، مما يشكل طمسًا للحدود بين مشاركة الدولة والقاعدة الشعبية [13].

توّفر عمليات الإنفاذ التي تتخذها المنصة والتقارير الصحافية الاستقصائية المزيد من الأدلة على هذا النظام البيئي الهجين. إذ أنه بين 2019 و 2020، فككت «ميتا» (فيسبوك) عددًا من شبكات السلوك المُنسّق غير الموثوق الصادرة من إسرائيل والتي استهدفت الجماهير في أفريقيا، أمريكا اللتينية وجنوب شرق آسيا، علمًا أن بعضها كان ذي ارتباط بالشركة الخاصة «أرخميدس جروب» ومقرها إسرائيل]31، 66[. وفقًا لتحقيق «ميتا»، القائمون على هذه الشبكات ارتكزوا على حسابات مُزيّفة لادارة الصفحات، نشر وتوزيع المحتوى، وتضخيم المشاركة بشكل مُصطنع. وقاموا دوريًا بالتعريف عن أنفسهم كفاعلين محليين رغم عدم صحة ذلك، ونشروا أخبارًا سياسية وصيرورات انتخابية، مما يعكس الجهود المُنظمة والمنهجية للتأثير على الخطاب السياسي وإخفاء مصدر العمليات وتنسيقها [31].

2.2.2 الـ«هسبارا» (الدعاية) الإسرائيلية

لأجل فهم التنظيم، استمرار ومثابرة، والمنطق الاستراتيجي القائم على التضليل الإعلامي الإسرائيلي وجهودها للتأثير المعلوماتي، من الضروري وضع هذه المُمارسات في السياق الأوسع للتقليد المُتبع في الدبلوماسية الاسرائيلية العامة المعروف باسم الـ«هسبارا». غالبًا ما يوصف الإعلام الاستراتيجي الاسرائيلي كـ«هسبارا» – وهي اصطلاح باللغة العبرية يُترجم عامة كـ«شرح» وبالعموم يُعنى بالجهود الدبلوماسية العامة، ويُقصد به الجهود طويلة الأمد لتشكيل وصياغة التصوّرات الدولية عن إسرائيل.

وبينما يُؤطر مسؤولون إسرائيليون الـ«هسبارا» بوصفها مُمارسة حيادية عبارة عن «شرح موقف إسرائيل» للجماهير الأجنبية، يُشدد باحثون ناقدون على الأبعاد السياسية والأيديولوجية الفكرية فيها [8، 61]. لم يصنف الباحثون الدعاية (هسبارا) الإسرائيلية على أنها دبلوماسية عامة تقليدية، بل كمشروع تواصلي إعلامي تديره الدولة بغية إدارة ومواجهة الانتقادات الدولية الموجهة لإسرائيل، لا سيما فيما يتعلق بحق الفلسطينيين في تقرير مصيرهم [8، 61].

في العصر الرقمي شهدت هذه المُمارسات تحوّلات مُعتبرة، مما دفع أوراغ ليطلق عليها اسم «هسبارا 2.0» (الدعاية 2.0) [8]. ويعكس هذا التحوّل التأقلم التكنولوجي من إعلام مطبوع ومرئي تقليدي إلى وسائل التواصل الاجتماعي والمنصات الرقمية واستفحال وتعاظم منظومة الدبلوماسية العامة الإسرائيلية]8[. عقب انتقادات وتقييمات نقدية لأداء إسرائيل الإعلامي أثناء حرب لبنان الثانية عام 2006 والصراعات اللاحقة في غزة، تعاملت مؤسسات الدولة والجيش الإسرائيلية بشكل متزايد مع التواصل الخارجي باعتباره مجالًا استراتيجيًا حيويًا، مما دفع إلى استراتيجية تواصل أكثر تنسيقًا واحترافية، حيث تم دمج إدارة الشرعية بشكل صريح في العقيدة العسكرية وتمت مواءمتها مع الجهود السياسية والقانونية والإعلامية. والأهم من ذلك، أن الأهداف الرئيسية للدعاية الإسرائيلية 2.0 (هسبارا 2.0) هي الرأي العام الأجنبي والنُخب السياسية، لا سيما في الدول الغربية التي يُعتبر دعمها الدبلوماسي والعسكري والمالي حيويًا [8].

الأهم من ذلك، أن هذه ليست مجرد ظاهرة تاريخية أو ظاهرة عابرة: فقد وسّعت إسرائيل بشكل ملحوظ الموارد المالية المخصصة لهذه الجهود. ففي ميزانية الدولة لعام 2026، خُصصت لوزارة الخارجية - إحدى الوكالات الرئيسية المعنية بالاتصال الخارجي والتواصل مع الأجانب – نحو 729 مليون دولار للدبلوماسية العامة وحملات الدعاية (الهسبارا)، أي أكثر من أربعة أضعاف الميزانية (نحو 150 مليون دولار) المُخصصة لأغراض مماثلة في عام 2025، وأكبر بكثير من ميزانيات ما قبل الحرب التي كانت قلة قليلة من مستويات الإنفاق الراهنة [64]. من المفترض أن يساهم هذا الالتزام المالي غير المسبوق بدعم حملات وسائل التواصل الاجتماعي الدولية، الشراكات مع المؤثرين، ورحلات وزيارات مسؤولين منتخبين أجانب وقادة المجتمع المدني إلى إسرائيل، مما يوضح نطاق مأسسة هذا النوع من التواصل الاستراتيجي [64].

يُبرز نطاق هذه المبادرات وحرفيتها أن النفوذ والتأثير يُمارس بشكل متزايد ليس من خلال القنوات الرسمية فحسب، بل أيضًا من خلال النبى التحتية الوسيطة للمنصات الرقمية التي تُمكّن وتُتيح الترويج مدفوع الأجر، والاستهداف المُتقدم للجماهير، والتلاعب الخوارزمي. تُعدّ هذه الديناميكيات ذات أهمية خاصة للدراسة الحالية، التي تُركّز على التضليل الإعلامي عبر جوجل، وخاصةً كيف يُمكن للمعلومات المُضلّلة الاستراتيجية أن تنتشر عبر إعلانات جوجل. ولذلك، يتناول القسم التالي جوجل كفاعل في البيئات المعلوماتية المعاصرة، من خلال أنظمة الإعلان والبحث الخاصة به.

2.3 جوجل كبنية تحتية للظهور السياسي والتأثير

يُحلل القسم الراهن دور جوجل في تشكيل الوصول إلى المعلومات والظهور السياسي. ويناقش بادئ ذي بدء تأثير مُحركات البحث، ومن ثم يعاين المنطق القائم على المناقصات لاعلانات جوجل (Google Ads)، قبل أن يستطرد في استكشاف كيفية توظيف الإعلان بنتائج البحث لتفكيك معلومات مُضللة أو مشكوك في صحتها، بما في ذلك حالات مُوثقة لحملات الحكومة الإسرائيلية.

2.3.1 الدور المؤثر لجوجل ومُحركات البحث

يُعدّ محرك بحث جوجل (Google Search) وسيطًا مُهيمنًا بين المستخدمين والمعلومات المتاحة عبر الإنترنت، حيث يُشكّل ما يتمّ التعرّف عليه، والوثوق به، والتعامل معه في صيرورة المنطقة السياسية اليومية]50[. تُظهر بيّنات ودلائل المسح هيمنة جوجل طويلة الأمد في صفوف مُستخدمي البحث [60]. بما أن المستخدمين يميلون لاعتبار النتائج المُصنفة عاليًا كذات مصداقية أكبرة وذات صلة أعلى بموضوع البحث، من شأن الترتيب والمرئية (الظهور) على مُحركات البحث أن تشكّل وتبني أحكامًا وخيارات لاحقة [55]. تُشير أبحاث تجريبية إلى أن الترتيب البحثي المُتحيّز قادر على تغيير تفضيلات المُصوّتين الذين لم يحددوا موقفهم بعد، مما يوحي بعواقب سياسية مُحتملة وقابلة للقياس للترتيب البحثي حتى من دون تغيير النظام البيئي القائم للمحتوى [26].

يُضخم حجم نطاق جوجل هذه التأثيرات: كشفت جوجل أنها تُعالج الآن أكثر من 5 ترليون بحث سنويًا [35] وهذا أمر مهم لدراسة التضليل الإعلامي لأن البحث ليس محض مؤشر غير فعّال على الانترنت؛ بل إنه منفذ كبير الحجم، عالي الثقة،

بالإمكان من خلاله اكتشاف السرديات السياسية، تعزيزها وتأكيدها، أو إدراجها بشكل استراتيجي في لحظات عدم اليقين أو الأخبار العاجلة [50].

2.3.2 إعلانات جوجل (Google Ads): ظهور قائم على المزايدة والنموذج التجاري القائم على الاهتمام

لا يزال نموذج إيرادات جوجل الجوهري عميق الارتباط بالإعلان. يُشدد تقرير «ألفابيت» (الشركة الأم لجوجل) السنويّ على أن إيرادات «خدمات جوجل» تعتمد بالأساس على الاعلانات المعروضة على «بحث جوجل» والأصول الإضافية أمثال «يوتيوب» [6]. في محرك بحث جوجل، يُنظم الظهور من خلال نظام مزايدة يتنافس فيه المعلنون للظهور في البحث عن استعلامات مُحددة؛ ولا يعتمد موضع الإعلان على العروض المقدمة فحسب، بل أيضًا على مؤشرات الملاءمة والجودة التي تحددها المنصة]32[. بالتالي، بالإمكان ترجمة قدرة الدفع للمرئية والظهور لحظة بحث المُستخدم عن معلومات بشكل مُباشر. يُعدّ منطق المزايدة هذا مهمًا لبحثنا لأنه يوّفر آليةً تمكّن الفاعلين السياسيين من شراء الانتباه وتوجيه التفسير، حتى عندما يبحث المستخدمون عن مصادر محايدة أو مؤسساتية (مثل الوكالات الإنسانية)، إذ يمكن ملء الجزء العلوي من الصفحة برسائل دعائية تُؤطّر ما سيقرأه المستخدم [75]. جدير بالذكر، أن الأبحاث في علم النفس المعرفي والإعلام السياسي تُظهر أن التعرض المبكر للمعلومات يُؤثر بشكل كبير على الأحكام والذاكرة. فعندما يُصادف المستخدم محتوىً مُضللًا أو مُؤطّر استراتيجيًا بالإمكان أن يشكل هذا المُحتوى كنقطة انطلاق أو مخطط ذهني للمعلومات اللاحقة، ليُشكّل ويصوغ الانطباعات حتى عندما يُصادف المستخدمون لاحقًا مواد تصحيحية أو ناقضة [52، 45]. يُعتبر تأثير الأسبقية هذا ذا أهمية خاصة في بيئات البحث، حيث غالبًا ما يقوم المستخدمون بمسح النتائج الأولى فقط وقد لا يميّزون بنظرة نقدية بين المحتوى المدعوم والمحتوى العضوي، مما يسمح للأطر الأولية السابقة بالبقاء ضمنيًا والتأثير على التصوّرات غير الواعية [55، 26].

2.3.3 المعلومات المُضللة والتضليل الإعلامي في إعلانات البحث عبر جوجل

يحلل ميتاكسا وتوريس – اتشيفيري عمليات البحث والاستفسار المعنية بالمرشحين في سياق الانتخابات الأمريكية للعام 2016، ويُشيرون إلى أن جزءًا مُعتبرًا من نتائج البحث الخاصة بالمُرشحين من المحتمل أن تكون مُحتوى مُزيّف أو مُنحاز، في دلالة على هشاشة البيئات المعرفية المتأثرة بالبحث أثناء فترة انتخابية [50]. وبالعموم، تُجادل الأبحاث المعنية بالاقتصادي السياسي للتضليل الإعلامي أن أسواق الاعلان الرقمية قادرة على تحفيز وتشجيع أو دعم المحتوى المُضلِل من خلال الانتفاع من الانتباه وتوجيه الموارد نحو الجهات الفاعلة القادرة على تحقيق أقصى قدر من الوصول [21]. وتُظهر أدلة ذات صلة أن أنظمة الإعلان قادرة على توفير الدعم المادي لسلاسل توريد المعلومات المُضللة، مما يُبرز كيف تتقاطع الحوافز التجارية مع سلامة المعلومات [1].

نظام الإنفاذ في إعلانات جوجل قائم على فئات السياسة والأحكام. في إطار سياسة جوجل المعنية بالتشويه والتحريف، من المُحتمل أن تقوم جوجل بتعطيل أو توقيف مُعلنين إذا ما حددت أن المُعلن المعني أو الهدف هو مُضلل أو مُخادع، بناء على مراجعة الاعلانات، المواقع، الحسابات، والمصادر من طرف ثالث [33]. تحظر سياسة جوجل نشر إعلانات تعمد إلى تضليل المستخدمين عبر حذف المعلومات ذات الصلة عن مُنتجات، خدمات، أو مصالح تجارية؛ وتحظر نشر إعلانات تسيء

تمثيل علاقات مع هيئات أو أجسام أخرى؛ وإعلانات توّفر أسعار مُضللة أو عروض غير مُتوّفرة؛ كما تحظر نشر إعلانات توّظف تصميم مُضلل أو خادع يشوّش أو يُغطي طبيعة الإعلان أو النيّة القائمة منه [33]. كما تحظر المُمارسات المُضللة والمُخادعة المُنسّقة في سياق سياسي أو سياقات قضايا مُجتمعية، كالتكتم عن أصل أو مصدر المُعلن عند استهداف مُستخدمين في دول أخرى [33]. تُعتبر الإنتهاكات لهذه السياسة شنيعة وقد تؤول إلى الحظر الفوري للحساب المُعلن عبر إعلانات جوجل وليس فقط رفض الإعلان نفسه، بالذات حينما تعرّض المعلومات المُضللة المستخدمين للأذى المحسوس أو الضرر الفعلي [33]. بشكل مُنفصل، تحتفظ جوجل بسياسة خاصة بالمحتوى ذات الطابع السياسي والتي تُعرّف وتُنظم «الاعلانات الانتخابية» في العديد من البُلدان والدول بواسطة التحقق من صحتها، بيانات عدم المسؤولية، وغيرها من المتطلبات [34].

وهذا أمر مهم على صعيد التحليل نظرًا لاحتمال أن تترتب على أي حملة دعائية أو إعلانية مدعومة من قبل حكومة ما عواقب سياسية من دون أن تكون متوافقة مع تعريفات «إعلانات انتخابية» بحسب جوجل. على سبيل المثال، الإعلانات التي تهاجم مصداقية إحدى وكالات الأمم المتحدة أو تنفي التقارير عن المجاعة والتي من شأنها أن تلعب دورًا في صياغة وتشكيل الآراء حول الحرب وتحمل المسؤولية عن الشؤون الإنسانية من دون أن تشمل بالضرورة جهات، أحزاب، مرشحين أو اعلانات ذات علاقة بالانتخابات، وبالتالي من المحتمل أن تعاملها المنصة كإعلانات عادية عوضًا عن إخضاعها للحوكمة كإعلانات ذات طابع سياسي في إطار سياسة جوجل للاعلانات الانتخابية [34، 65].

2.3.4 إعلانات الحكومة الإسرائيلية عبر إعلانات جوجل

حالة الأونروا - وكالة غوث وتشغيل اللاجئين الفلسطينيين

يُقدّم التقرير الاستقصائي مثالًا ملموسًا على المفعول الذي يمكن أن تحمله الرسائل الحكومية عبر إعلانات بحث جوجل. ففي عام 2024، أفادت مجلة WIRED بأن دائرة الإعلان الحكومية الإسرائيلية قد إقتنت إعلانات بحث جوجل للظهور في عمليات البحث عن «الأونروا» (UNRWA) و»الأونروا الولايات المتحدة» (UNRWA USA) باللغة الانجليزية، موجهةً المستخدمين إلى موقع الكتروني حكومي يعرض مزاعم تهدف إلى تقويض الثقة في الوكالة [75]. ويصف التقرير كيف استهدفت هذه الاستراتيجية نوايا المانحين (أي عمليات البحث التي يجريها الأشخاص الذين يبحثون عن المنظمة) واستغلت صفحة البحث لنشر معلومات مُضللة عن شرعية الوكالة [75]. وبموجب الأرقام الواردة في التقرير، فقد ظهرت الإعلانات المرتبطة بإسرائيل في المئات من عمليات البحث المتعلقة بالأونروا، وفي قسط كبير من الوقت حينما استوفت الشروط؛ وتحديدًا في الفترة الواقعة بين أيار/ مايو وتموز/ يوليو، ظهرت الإعلانات المرتبطة بإسرائيل في 44% من الحالات التي استوفت فيها إعلانات مرتبطة باسرائيل وإعلانات الأورنوا الولايات المتحدة (UNRWA USA) شروط أهلية العرض، في حين ظهرت إعلانات الأونروا الولايات المتحدة (UNRWA USA) في 34% فقط من تلك الحالات المؤهلة، مما يوضح كيف يمكن للظهور المدفوع أن يتفوق على الرسائل الدعائية الخاصة بالمنظمة المعنية [75].

وقد جادلت الشكاوى أن الإعلانات كانت مُضللة واستخدمت علامة تجارية مرتبطة بالأونروا بشكل يُحدث الارباك. وقد كانت نسخ سابقة من الحملة الدعائية صريحة للغاية: وفقًا لـ «WIRED»، روّجت إسرائيل إعلانات جوجل في الولايات المتحدة تزعم

أنه «لا يمكن فصل الأونروا وحماس» وأن الوكالة «تواصل توظيف الإرهابيين»، وهي رسائل تخشى وكالة غوث وتشغيل اللاجئين الفلسطينيين – الأونروا أن تؤثر في الرأي العام بالذات في وقت مورست فيه ضغوط على السياسة الأمريكية والدعم المادي للأونروا [75].

عقب رفع الشكاوى بادئ الأمر، أزالت جوجل بعض هذه الإعلانات؛ إلا أن إسرائيل عاودت تحديث حملتها في وقت لاحق مستخدمة إصطلاحات مُعدلة. وتُظهر لقطات شاشة راجعتها «WIRED» إعلانات مُروّجة تحت عناوين مثل «حيادية الأونروا مُنتهكة»، «إسرائيل تكشف مشاكل بالأونروا»، و «إسرائيل تدعو للممارسات أكثر شفافية وأمانًا»، في تلطيف للغة يُوّجه المُستخدمين لاتهامات مشابهة بالعموم [75]. وتُفيد التقارير أن جوجل أخذت الموقف القائل إن الإعلانات لم تنتهك سياساتها، ولم تنتهك تحديدًا سياسة «ادعاء ادعاءات كاذبة صراحة والتي من شأنها أن تقوّض إلى حدٍ كبير المشاركة أو الثقة في العملية الانتخابية أو الديمقراطية.» واستخدام العلامات التجارية وماركات شخص آخر «بشكل مُحدث للإرباك، مُضلل أو مُخادع». قد يُفهم من هذه الحلقة أن الادعاءات السياسية الجدلية قد تستمر وتبقى في مخزون البحث مدفوع الأجر عمليًا حينما يتم تأطيرها كمرافعة أو نقد عوضًا عن كونها وقائع جازمة قابلة للتحقق من صحّتها والتي تتسبب بإنفاذ التشويه والتحريف، حتى حينما لا يتم تغيير السردية المُضمنة والأساسية [33، 75].

حالة مجاعة غزة

أشارت الواشنطن بوست عام 2025 إلى شكاوى داخلية تُعنى بإعلانات الحكومة الإسرائيلية عبر يوتيوب وجوجل والتي زعمت «يوجد طعام في غزة» ورفضت المجاعة مُشيرة إلى انحياز إعلامي؛ علمًا أن جوجل خلصت إلى أن هذه الاعلانات لم تنتهك سياساتها [65]. وقد وصفت تغطية إعلامية موازية صرف مخصصات مالية (تُدّر بـ45 مليون دولار أمريكي) على حملات من هذا النوع وتأطيرها كجهود نشر معلومات عامة متسّقة عبر البنى التحتية لإعلانات جوجل [69، 22].

3. المناهج

يصف هذا الفصل صيرورات تجميع البيانات والنهج التحليلي المُستخدم في هذه الدراسة. ويصف بالتفصيل مبنى قاعدة البيانات، التصنيف اليدوي لموضوعات الإعلانات، إعادة هيكلة البيانات لغرض التحليل، والمنهجيات المُستخدمة لتقييم الانكشاف والتعرّض لكل إعلان وإعلان. ويُختتم الفصل باستعراض موجز لأمثلة توضيحية عن تلك الإعلانات.

3.1 جمع البيانات

تعتمد هذه الدراسة على بيانات الإعلان التي قام مركز الشفافية لاعلانات جوجل بجمعها. جمعنا جميع الإعلانات التي نشرها إثنان من المُعلنين، «دائرة الإعلانات الحكومية الإسرائيلية» و»وكالة الإعلانات التابعة لحكومة إسرائيل» في نطاق المنطقة الاقتصادية الأوروبية (EEA) وتُركية. تم جمع البيانات يوم 15 تشرين الأول/ أكتوبر 2025، وتُعنى البيانات بالفترة المُمتدة بين 22 آذار/ مارس 2025

و14 تشرين الأول/ أكتوبر 2025، وتشمل معلومات عن المُعلنين والإعلانات الفردية. تشمل قاعدة البيانات المُجمعة التي يُطلق عليها اسم «لائحة الإحصائيات الإبداعية» (the creative_stats table): معلومات على صعيد الجهة المُعلنة: الاسم القانوني، الإسم المُعلن، حالة التحقق، الموقع

معلومات على صعيد الإعلان: نطاقات الانطباع بحسب المنطقة (يشمل العدد الإجماليّ للانطباعات في المنطقة الاقتصادية الأوروبية)، أول وآخر موعد للعرض، هيئة الإعلان (فيديو أو صورة مثلًا)، التصنيف الموضوعيّ بحسب ما توّفره المنصة، معايير استهداف الجماهير، إذا ما كان تم تمويل الإعلان عن طريق برنامج مِنح إعلانات جوجل، رابط مُباشر للإعلان (creative_page_url)

تتضمن مجموعة البيانات فئة إجمالية خاصة بالمنطقة الاقتصادية الأوروبية (EEA). ونظرًا لأن الملاحظات على مستوى المنطقة الاقتصادية الأوروبية تمثل بيانات مُجمّعة عبر عدة دول، فإن إدراجها إلى جانب المناطق الفردية كان سيؤدي إلى احتساب الإعلانات بشكل مزدوج. ولتفادي هذه الإشكالية، تم استبعاد جميع الملاحظات المتعلقة بالفئة المجمّعة للمنطقة الاقتصادية الأوروبية من التحليل. وتشمل مجموعة البيانات المستخدمة في التحليلات اللاحقة 1,220 تصميمًا إعلانيًا فريدًا و7,359 حالة إعلان منشور (منها 6,916 صادرة عن "وكالة الإعلانات الحكومية الإسرائيلية" و443 صادرة عن "دائرة الإعلانات الحكومية الإسرائيلية") عبر مختلف المناطق ومنصات العرض (بما في ذلك البحث، والخرائط، والتسوّق، ويوتيوب). وتعود جميع الإعلانات إلى مصادر في إسرائيل.

3.2 التصنيف اليدوي لموضوعات الإعلانات

بهدف تمكين تحليل موضوعاتيّ (قائم على التيمات) أكثر دقة، قمنا بتصنيف كل تصميم إعلانيّ فريد يدويًا. على أن يشمل كل إعلان:

1. تم الولوج إلى الصفحة التصميمية الإبداعية creative_page_url المواتية .
2. تمت مراجعة المُحتوى (فيديو، صورة، أو نص) وترجمته حسب الحاجة.
3. جرى إسناد تصنيف موضوعاتي (تيماتيّ).

من أصل 1,220 تصميمًا إبداعيًا، جرى إسناد تصنيف موضوعاتي بنجاح لـ 1,211 إعلانًا (يشكّلون 99,3%). لم يفلح الولوج إلى عدد صغير من الإعلانات إثر رابط غير سليم أو محتوى غير مُتوّفر، وبالتالي تبنينا التحويلات التالية: أ) الإعلانات التي لم يفلح الوصول إليها تم تصنيفها كـ«لاغية»؛ ب) الإعلانات ذات محتوى الفيديو غير المُتوّفر تم تصنيفها كـ «فيديو غير مُتوّفر»؛ ج) فقط عندما توّفر عنوان الإعلان وتم استنباط الموضوع (إن كان مُباشرة من العنوان أو عن طريق مُقارنته بإعلانات شبيهة ذات مُحتوى معروف). على سبيل المثال، أسند تصنيف «توزيع المساعدات في غزة» إلى إعلان بعنوان «الوجوه السعيدة لا تكذب، حماس تكذب»، بناء على ظهوره المُكرر في إعلانات أخرى مرتبطة بوضوح بهذا الموضوع.

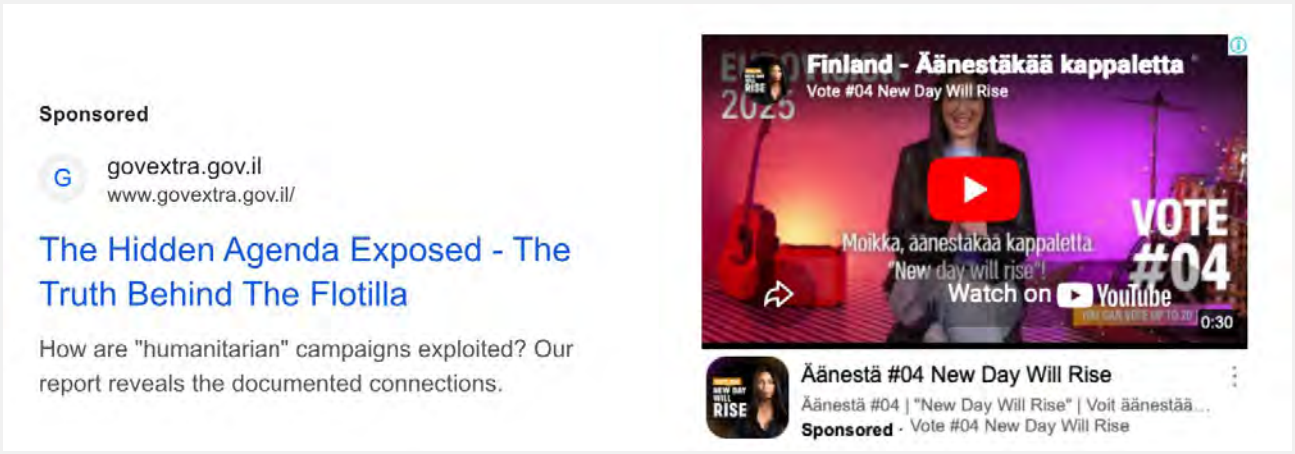
3.4 قياس التعرّض للإعلانات

تُعرض بيانات مرات الظهور (Impressions) على شكل نطاقات دنيا وعليا. وقد تم تقدير مستوى التعرّض باستخدام القيمة الوسطية بين هذين الحدّين. ولإلتقاط الديناميكيات الزمنية، تم توسيع الفترة الزمنية لنشاط كل إعلان إلى لوحة بيانات يومية، مع افتراض توزيع متساوٍ لمرات الظهور عبر الأيام التي كان فيها الإعلان نشطًا.

وبما أن بيانات مرات الظهور تُتاح للعامة مع تأخير مدته 90 يومًا لأسباب تتعلق بالخصوصية، فقد أُجري جمع بيانات ثانٍ بعد انقضاء هذه الفترة لاستكمال بيانات مرات الظهور الناقصة لأحدث الملاحظات. تضمن هذه الإجراءات تغطية أكثر اكتمالًا لمستوى التعرّض عبر كامل فترة الدراسة.

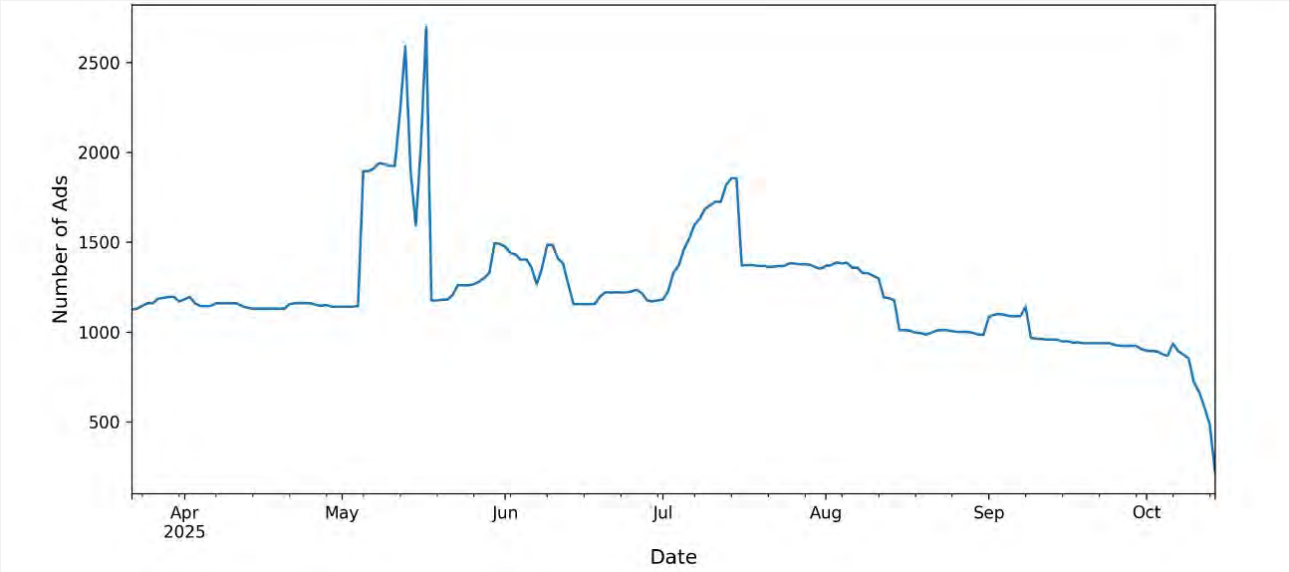
3.5 بعض الأمثلة لإعلانات

يستعرض هذا القسم أمثلة تمثيلية لأنواع الإعلانات المُدرجة في مجموعة البيانات. كما يظهر في الرسم 1 والرسم 2، قد تكون الإعلانات على هيئات مختلفة في نظام إعلانات جوجل البيئيّ، قائمة على النص، قائمة على الصورة، وقائمة على الشريط المُسجّل (فيديو). عادة ما تتكوّن الإعلانات القائمة على النص من رسائل نصيّة قصيرة تهدف إلى نقل معلومات أو توجيه المُستخدمين إلى مُحتوى خارجيّ، في حين أن الإعلانات القائمة على الشريط المُسجّل (الفيديو) تدمج عناصر مرئية وصوتية لنقل سرديات أكثر استفاضة. تُبرز هذه الأمثلة تنوّع الهيئات المُستخدمة لتوزيع ونشر الرسائل، مما يحمل عواقب على كيفية تأطير المعلومات وكيف يُدركها المُستخدمون.



الرسم 1: إعلان قائم على النص.

الرسم 2: إعلان قائم على الفيديو
.



الرسم 3: إعلانات نشطة لليوم (22 آذار/ مارس 2025 – 14 تشرين الأول/ أكتوبر 2025

4. النتائج

يعرض هذا الفصل النتائج التجريبية (الأمبيرية) للدراسة. يبدأ باستعراض بنظرة عامة على مجموعة بيانات إعلانات جوجل، يشمل مستويات النشاط، الهيئات والأشكال، والتوزيع الجُغرافيّ. ومن ثم يتناول الهيكلية الموضوعاتية للإعلانات وديناميكياتها الزمنية، قبل تقديم تحليل نوعي لإعلان مُختار.

4.1 نظرة عامة عن مجموعة بيانات إعلانات جوجل

يُقدّم هذا القسم نظرة عامة توصيفية لمجموعة البيانات. ويُعاين حاصل النشاط الإعلانيّ، توزيع الإعلانات عبر منصات العرض والهيئات، أنماط الاستهداف الجُغرافي وفئات التصنيف الموضوعيّ التي حددتها المنصة.

4.1.1 حاصل النشاط الإعلاني

يستعرض الرسم 3 العدد اليوميّ لمُعاينات الإعلانات النشطة بين 22 آذار/ مارس 2025 و 14 تشرين الأول/ أكتوبر 2025. يُبيّن النمط الزمانيّ عدّة مراحل مُتميّزة ومُكثّفة للحملة بدلًا من توزيع منتظم على وقت مطوّل. فبعد مستوى أساسي معتدل نسبيًا في أواخر آذار/ مارس ونيسان/ أبريل 2025 (نحو 1,100 – 1,200 إعلان نشط)، يزداد النشاط بشكل حاد في أوائل أيار/ مايو، ليصل لذروة تتجاوز الـ 2,500 إعلان نشط. إلا أن هذه الزيادة لم تدم مُطوّلًا، إذ انخفضت المستويات إلى نحو 1,200 بعدها بوقت قصير.

واتسمت الأسابيع التالية بتذبذات مُعتدلة، مع زيادة فرعية ملحوظة في حزيران/ يونيو وزيادة أشدّ مطلع تموز/ يوليو، حين اقترب النشاط من مستويات أعلى قبل الاستقرار. وبدءًا من آب/ أغسطس فما بعد، يتراجع عدد الإعلانات النشطة تدريجيًا لينخفض دون حد الألف إعلان بحلول أيلول/ سبتمبر.

بالمُجمل، يُشير النمط إلى دفعات عرضية من النشاط الإعلانيّ المُعزّز منثورة بفترات من الاستقرار النسبي، مما يدل على أن الحملة انتهجت العمل بموجات مُركزّة عوضًا عن النشر المتواصل على نطاق واسع. من الواجب تحليل التراجع المُبيّن والصريح في أواخر فترة المُعاينة بحذر، إذ أن البيانات التي تم جمعها في الـ15 من تشرين الأول/ أكتوبر 2025 ونظام شفافية الإعلانات قد لا تعكس جميع الإعلانات النشطة في حينه نظرًا للتأخيرات في التبليغ (التي تحتاج بين 48 و 72 ساعة بالعادة).

الرسم 4: التوزيع الجغرافي للاعلانات (المراتب الـ15 الأولى)

4.1.2 توزيع منصات العرض والهيئات

كما هو موضح في الجدول 1، يتسم توزيع منصات عرض الإعلانات بتركيزٍ مرتفع، حيث تستحوذ منصة يوتيوب على الغالبية العظمى من مرات الظهور المقدّرة، إذ تمثل 98.68% من إجمالي مرات الظهور. في المقابل، تسهم المنصات الأخرى بشكل هامشي أكثر في الحملة الإعلانية، حيث تمثل الإعلانات عبر البحث (Search) 0.60%، بينما تشكل الخرائط (Maps) ومتجر التطبيقات (Play) والتسوّق (Shopping) نسبة 0.24%.

المنصة	مرات الظهور المقدرة	النسبة (%)
YouTube	283,218,500	98.68
Search	1,714,500	0.60
Maps	688,500	0.24
Play	688,500	0.24
Shopping	688,500	0.24

وفيما يتعلق بصيغة الإعلان، تُعدّ الإعلانات المصوّرة (فيديو) الصيغة المهيمنة بنسبة 70.1%، تليها الإعلانات النصية بنسبة 24.5%، ثم الإعلانات الصورية بنسبة 5.4%. ويتسق هذا التوزيع مع تركز مرات الظهور على منصة يوتيوب، ما يشير إلى اعتماد المعلنين بشكل أساسي على الصيغ المعتمدة على الفيديو لتعظيم الوصول والتفاعل، في حين لعبت الإعلانات النصية والصورية دورًا أقل أهمية عبر المنصات الأخرى.

4.1.3 التوزيع الجُغرافيّ

يكشف التوزيع الجُغرافيّ للإعلانات عن بصمة حملة أوروبية بالعموم، مع انكشاف يغطي متنوّعًا واسعًا من السياقات الوطنية. على صعيد البيانات المُعاينة، تحتل اليونان (8,7%) الحصة الأكبر من الانكشاف للاعلان، تليها ألمانيا (8,0%) وبلجيكا (7,5%). كما حظيت قبرص (5,9%)، فرنسا (5,5%) والنمسا (5,3%) بحصة لا بأس بها من التعرض للاعلان، مما يُشير إلى حضور قوي في المناطق الوسطى الأوروبية والضواحي. الحلقة التالية من الدول التي عُرضت فيها الاعلانات تشمل هولندا (5,0%)، الدانمارك (4,5%)، إيطاليا (4,1%)، جمهورية التشيك (4,0%)، وإيرلندا (4,0%) مع مستويات انكشاف عالية نسبيًا. كما تمت مُعاينة نسب صغيرة، لكن مُعتبرة في كل من لوكسمبورغ (3,1%)، بولندا (3,0%)، ليتوانيا (2,9%)، وفنلندا (2,7%). بالعموم، يُشير التوزيع على استراتيجية استهداف مُوّزعة جُغرافيًا، من دون أن تهيمن دولة ما على الحملة.

في حين يعكس هذا النمط مشاركة إقليمية واسعة النطاق عوضًا عن التركيز على عدد قليل من الأسواق، من الجدير ملاحظة إدراج اليونان وقبرص ضمن أبرز المتلقين للاعلانات على ضوء التطوّرات الاجتماعية والجيوسياسية الأخيرة في شرق المتوسط. على خلفية تصاعد التوترات الإقليمية، لا سيما في أعقاب حرب الـ12 يومًا بين إسرائيل وإيران في 2025، حيث أشارت تقارير الى تدّفق من التقارير المُعتبرة عن الانتقال إلى بلاد أخرى. حيث تُفيد تقديرات إخبارية حديثة إلى أن نحو 10,000 إسرائيلي انتقلوا إلى اليونان منذ تشرين الأول/ أكتوبر 2023 [19]. وبالمثل، إستقبلت قبرص نحو 15,000 مواطن إسرائيلي مؤخرًا، مع زيادة مُعتبرة باقتناء العقارات ونشاط استيطاني طويل الأمد]18[. على صعيد الدول، تتقاطع هذه المقاربة الاجتماعية مع تعميق التعاون المؤسساتي. إذ وقّعت إسرائيل واليونان وقبرص أواخر 2025 على اتفاق خطة عمل عسكرية ثلاثية للعام 2026 تسعى لتكثيف التدريبات العسكرية المُشتركة وتعزيز التنسيق الأمني في شرق المتوسط [59]. يُضفي تقارب موجات الهجرة والتعاون الأمني الرسمي أهمية سياقية إضافية لتبوأ هذين البلدين مواقع متقدمة في إطار استراتيجية الاستهداف الجغرافي للحملة.

4.1.4 فئات التصنيف الموضوعيّ التي حددتها المنصة

يُظهر التوزيع الموضوعي للإعلانات (الجدول 2) تركيزًا كبيرًا في فئة القانون والحكومة، التي توازي 81,9% من مُحصلة الإعلانات. أما الفئات المتبقية فتمثل حصصًا هامشية فقط من الحملة. علمًا أن الفئات الأكثر شيوعًا بعد القانون والحوكمة بالترتيب، هي الفنون والترفيه (4,2%)، والأخبار والكتب والمنشورات (3,2%)، والوظائف والتعليم (2,4%)، أي أن كل منها يمثّل أقل من خمسة بالمئة من مُحصلة الإعلانات، بينما تبقى جميع التصنيفات الموضوعية الأخرى أدنى من اثنين بالمئة.

الجدول 2: توزيع موضوع الإعلانات (على مستوى التصميم الإبداعيّ)

فئة الموضوع	النسبة (%)
القانون والحوكمة	81.86
الفنون والترفيه	4.16
الأخبار والكتب والمنشورات	3.23
الوظائف والتعليم	2.35
البيت والحديقة	1.97
العائلة والمجتمع	1.97
الطعام والمُشتريات	1.83
الصحة	1.36
الرياضة واللياقة	0.41
السيارات والمركبات	0.27
ثياب	0.19
حواسيب وإلكترونيكيات	0.14
هوايات وألعاب ووقت الفراغ	0.14
شؤون مالية	0.08
الأعمال والصناعة	0.04

4.2 التصنيف الموضوعاتيّ (التيماتيّ) للإعلانات

يستعرض هذا القسم نتائج التصنيف الموضوعاتيّ (التيماتيّ) اليدوي. ويُوجز بداية الموضوعات المركزية المُشخّصة في مجموعة البيانات، قبل أن يتم تحليل تطوّرها الزمانيّ بموجب التقدير النسبي للانطباعات ونشاط الإعلان بمرور الوقت.

4.2.1 استعراض الموضوعات

من أصل 1,220 تصميمًا إبداعيًا فريدًا، تمكنا من إسناد تصنيف موضوعاتي لـ 1,211 إعلانًا (7,112 من أصل 7,359 مُعاينة). لأغراض التحليل اللاحق، قمنا باستبعاد الإعلانات التي لم نفلح في تصنيفها نظرًا لعدم توّفرها.

يمثل الجدول 2 توزيع الموضوعات المُصنفة يدويًا للاعلانات. تكشف النتائج عن توزيع شديد الانحراف، إذ تُشكل فئة «تصويت اليوروفيجن» قرابة نصف مُجمل الإعلانات (47,5%). وتتبع الفئة المُهيمنة مجموعة أصغر بكثير من الموضوعات، ولعل أبرزها «توزيع المساعدات في غزة» (13,3%) و«التأمين الوطني (بالعبرية)» (7,7%)، في حين بالكاد تبلغ الفئات المتبقة منفردة 6% من المُعاينات. بعد هذه الموضوعات التي تتبوأ الطليعة يصبح التوزيع مجزءًا بدرجة كبيرة جدًا مع قائمة طويلة من الفئات قليلة الاستخدام، والتي يمثّل معظمها ما لا يزيد عن 1% من مجموعة البيانات.

غير أن هذا النمط يختلف بشكل ملحوظ عند النظر إلى التعرّض الإعلاني. فعلى مستوى مرات الظهور المقدّرة، تبرز فئة "توزيع المساعدات في غزة" بوصفها الموضوع الأكثر بروزًا (38.7%)، متقدمةً بشكل طفيف على فئة "التصويت في مسابقة يوروفيجن" (36.9%)، رغم أن عدد الإعلانات فيها أقل بكثير. ويشير هذا التباين إلى أن الإعلانات ضمن فئة "توزيع المساعدات في غزة" كانت، في المتوسط، تُعرض بكثافة أعلى مقارنةً بتلك التابعة لفئة "التصويت في مسابقة يوروفيجن". وبالمثل، فإن بعض الموضوعات التي تضم عددًا محدودًا نسبيًا من الإعلانات— مثل "الأمم المتحدة ترفض توزيع المساعدات إلى غزة" أو "ادعاء عدم وجود غذاء في غزة كذبة"—تستحوذ على حصص غير متناسبة من إجمالي مرات الظهور.

وتسلّط هذه الفروقات الضوء على تمييز واضح بين حجم الإعلانات ومدى وصولها الفعلي. ففي حين تعتمد بعض الموضوعات على عدد كبير من التصاميم الإعلانية وحالات الظهور، تحقق موضوعات أخرى وصولًا مرتفعًا رغم عدد أقل من الإعلانات، ما يشير إلى تباين في شدة الحملات واستراتيجيات التوزيع بين مختلف الموضوعات.

4.2.2 الانطباعات الموضوعاتية بمرور الوقت

يعرض الرسم 5 التطوّر الزمانيّ للانكشاف للاعلانات بحسب موضوعات (تيمات)، والتي تُقاس بعدد مرات الظهور اليومية بالتقدير، معروضة على مقياس لوغاريتمي. يُقدر عدد الانطباعات كنقطة المُنتصف بين الحدين الأدنى والأعلى المُبلغ عنهما، ويتم توزيعها بالتساوي على مدار فترة نشاط كل إعلان.

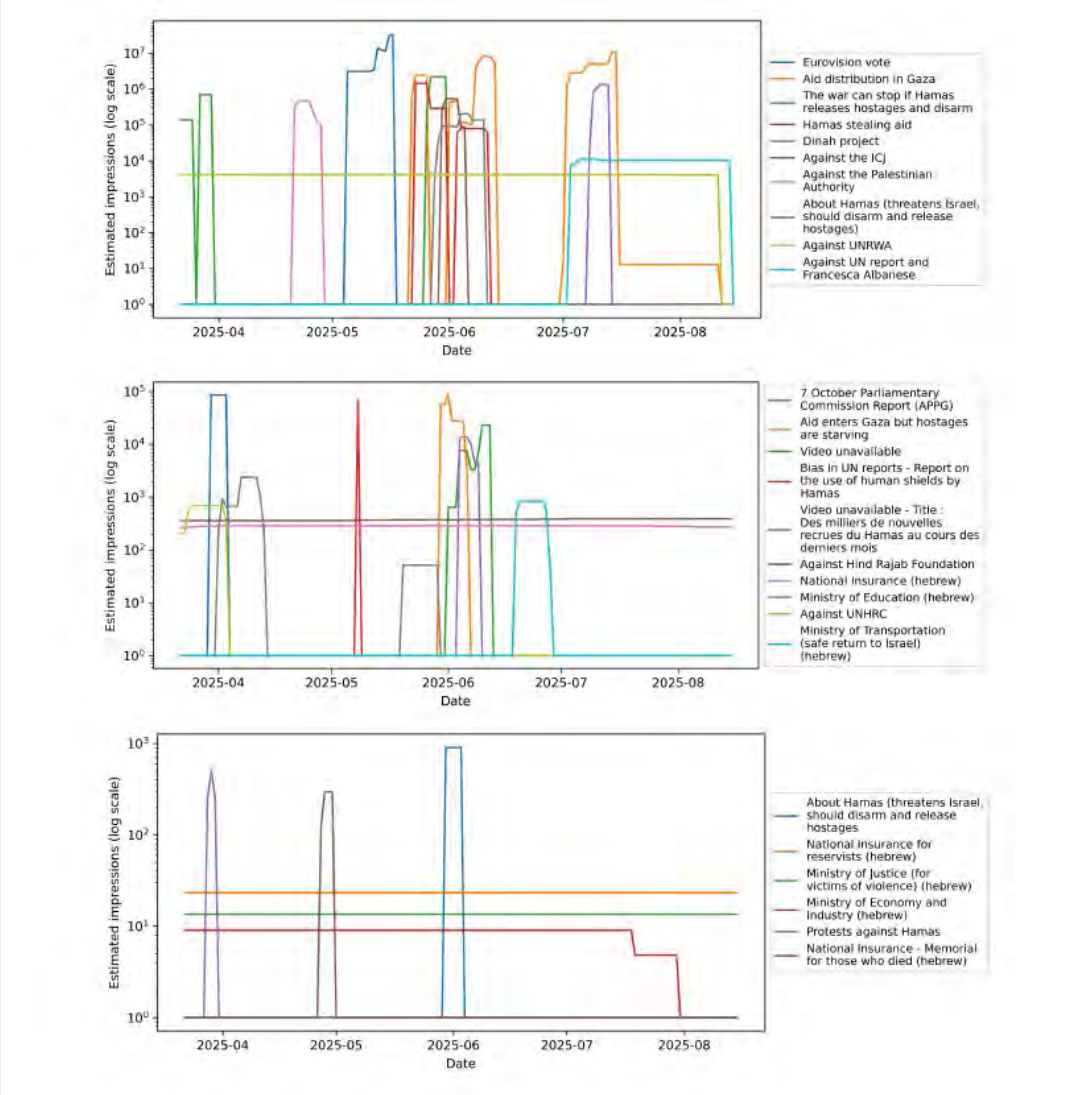
يعكس هذا التقييد سياسة الإبلاغ الخاصة بجوجل، التي تنشر بيانات الانطباعات في مركز شفافية الإعلانات بتأخير يقارب 90 يومًا لأسباب تتعلق بالخصوصية. ونتيجة لذلك، قد تحتوي المُعاينات الأقرب إلى تاريخ جمع البيانات على معلومات غير مكتملة أو مفقودة عن الانطباعات ومرات الظهور، ومن شأن استبعاد هذه الفترة أن يضمن تمثيلًا موثوقًا بدرجة أكبر للانكشاف على هذه الاعلانات بمرور الوقت. تكشف النتائج عن تباين كبير في الانكشاف على الاعلانات باختلاف الموضوعات وعلى مدار الوقت. تُشير نقاط الذروة في السلسلة الزمنية إلى فترات تكثيف النشاط الإعلاني، بينما يُبرز المقياس اللوغاريتمي الاختلافات بين الموضوعات ذات الانكشاف العالي والمنخفض. ولتسهيل القراءة، تُعرض الموضوعات بثلاث مجموعات بناءً على مستوى تعرضها الإجمالي.

يشير الرسم 5 إلى أن النشاط الإعلاني ليس غير متساوٍ بين الموضوعات فحسب، بل إنه أيضًا شديد الارتباط بالوقت، حيث تظهر معظم الموضوعات لفترات قصيرة ومركزة بدلًا من الانكشاف المتواصل. يُشير هذا النمط إلى أنه من المحتمل أن تكون المواضيع الفردية قد تم نشرها بشكل استراتيجي كرد فعل للأحداث أو اللحظات العينية في البيئة المعلوماتية. أوضح مثال على ذلك هو موضوع «تصويت اليوروفيجن»، والذي يبلغ الذروة بحدّة في الأسابيع السابقة لمسابقة الغناء الأوروبية – اليوروفيجن ويختفي مباشرة بعد انتهاءها، مما يعكس استراتيجية اعلامية مُرتبطة بالأحداث بشكل وثيق.

الجدول 3: توزيع موضوعات الغعلانات المُصنفة يدويًا

فئة الموضوع	Ads(%)	Creatives	Impressions(%)
توزيع المساعدات في غزة	953(13.40)	209	132,109,000(38.72)
تصويت مسابقة الغناء اليوروفيجين	3,380(47.53)	652	126,104,000(36.96)
الأمم المتحدة ترفض توزيع المساعدات في غزة	18(0.25)	18	19,534,500(5.73)
عدم وجود الأكل في غزة كذبة	25(0.35)	17	15,059,500(4.41)
بالإمكان وقف الحرب إذا حررت حماس الرهائن ونزعت سلاحها	100(1.41)	20	14,640,000(4.29)
حماس تسرق المساعدات	60(0.84)	12	7,878,500(2.31)
المجاعة في غزة هي كذبة	20(0.28)	20	6,872,000(2.01)
مشروع دينا	105(1.48)	21	5,904,500(1.73)
المساعدات تدخل إلى غزة لكن الرهائن يتضوّرون جوعًا	59(0.83)	15	3,895,500(1.14)
ضد محكمة العدل الدولية	90(1.27)	18	2,567,500(0.75)
ضد السلطة الوطنية	30(0.42)	6	2,550,000(0.75)
عن حماس (تهدد اسرائيل، يجب نزع سلاحها واطلاق سراح الرهائن)	165(2.32)	33	1,651,000(0.48)
ضد وكالة غوث وتشغيل اللاجئين – الأونروا	185(2.60)	19	584,500(0.17)
الرهائن جائعين في غزة	19(0.27)	15	511,500(0.15)
ضد تقرير الأمم المتحدة وفرانشيسكا ألبانيزي	235(3.30)	10	440,500(0.13)
تقرير لجنة التحقيق البرلمانية في أحداث السابع من أكتوبر (APPG)	5(0.07)	1	425,000(0.12)
فيديو غير متوّفر	65(0.91)	13	106,000(0.03)
وزارة الهجرة والإستيعاب	173(2.43)	25	97,500(0.03)
ضد مؤسسة هند رجب	390(5.48)	7	77,000(0.02)
الانحياز في تقارير الأمم المتحدة – تقرير عن استخدام حماس للدروع البشرية	10(0.14)	2	66,500(0.02)
فيديو غير متوّفر (مجندو حماس)	25(0.35)	5	59,500(0.02)
دعاية لفعالية بالعبرية	99(1.39)	9	58,500(0.02)
التأمين الوطني (بالعبرية)	545(7.66)	14	55,500(0.02)
توظيف في شرطة إسرائيل	68(0.96)	14	24,000(0.01)
وزارة التربية والتعليم (بالعبرية)	35(0.49)	5	17,500(0.01)
خلل في تقرير التصنيف المرحلي المتكامل للأمن الغذائي	7(0.10)	6	8,500(0.00)
ضد مجلس حقوق الإنسان التابع للأمم المتحدة	45(0.63)	2	7,500(0.00)
وزارة المواصلات (العودة الآمنة إلى اسرائيل - بالعبرية)	70(0.98)	1	7,000(0.00)

توظيف سجون إسرائيل (لغة عبرية)	20(0.28)	4	6,000(0.00)
التأمين الوطني لخادمي الاحتياط (بالعبرية)	45(0.63)	1	4,500(0.00)
برنامج عميت (لغة عبرية)	5(0.07)	1	2,500(0.00)
وزارة العدل (لضحايا العنف – بالعبرية)	20(0.28)	2	2,000(0.00)
برنامج عميت (لغة عبرية)	2(0.03)	1	1,000(0.00)
بنك إسرائيل	6(0.08)	2	1,000(0.00)
سلطة الأراضي الإسرائيلية (لغة عبرية)	2(0.03)	2	1,000(0.00)
مظاهرات ضد حماس	10(0.14)	2	1,000(0.00)
وزارة الاقتصاد والصناعة (بالعبرية)	10(0.14)	1	1,000(0.00)
التأمين الوطني – ذكرى للقتلى (بالعبرية)	10(0.14)	1	1,000(0.00)
ضد أسطول كسر الحصار	11(0.15)	7	0(0.00)



الرسم 5: تقديرات للانطباعات اليومية بحسب الموضوع (مقياس لوغارثمي). تُعرض فقط الموضوعات ذات تغطية انطباعات (مرات ظهور) كافية (أي أكثر من 70% من المُعاينات غير الناقصة). تم تجميع الموضوعات لأجل تسهيل القراءة.

قائمة الموضوعات بالترتيب:

- تصويت اليوروفيجن
- توزيع المساعدات في غزة
- بالإمكان وقف الحرب إذا حررت حماس الرهائن ونزعت سلاحها
- حماس تسرق المساعدات
- مشروع دينا
- ضد محكمة العدل الدولية
- ضد السلطة الوطنية
- عن حماس (تهدد اسرائيل، يجب نزع سلاحها واطلاق سراح الرهائن)
- ضد وكالة غوث وتشغيل اللاجئين – الأونروا
- ضد تقرير الأمم المتحدة وفرانشيسكا ألبانيزي
- تقرير لجنة التحقيق البرلمانية في أحداث السابع من أكتوبر (APPG)
- المساعدات تدخل إلى غزة لكن الرهائن يتضوّرون جوعًا
- فيديو غير متوّفر
- الانحياز في تقارير الأمم المتحدة – تقرير عن استخدام حماس للدروع البشرية
- فيديو غير متوّفر (مجندو حماس)
- ضد مؤسسة هند رجب
- التأمين الوطني (بالعبرية)
- وزارة التربية والتعليم (بالعبرية)
- ضد مجلس حقوق الإنسان التابع للأمم المتحدة
- وزارة المواصلات (العودة الآمنة إلى اسرائيل - بالعبرية)
- عن حماس (تهدد إسرائيل، يجب أن تنزع سلاحها وتطلق سراح الرهائن)
- التأمين الوطني لخادمي الاحتياط (بالعبرية)
- وزارة العدل (لضحايا العنف – بالعبرية)
- وزارة الاقتصاد والصناعة (بالعبرية)
- مظاهرات ضد حماس
- التأمين الوطني – ذكرى للقتلى (بالعبرية)

ثمة مجموعة ثانية بارزة من الموضوعات التي تُعنى بالمجاعة والأوضاع الإنسانية في غزة. يظهر أن موضوع «توزيع المساعدات في غزة» شهد ذروات ملحوظة في صيف 2025، وهي فترة تميّزت بتزايد التقارير الدولية عن مخاطر المجاعة وانعدام الأمن الغذائي بشكل حاد المرتبط بالحصار المفروض على القطاع. وقد وثّقت منظمات مثل «التصنيف المرحلي المتكامل للأمن الغذائي» والأمم المتحدة هذه الديناميكيات على نطاق واسع، مُحذّرة من انعدام الأمن الغذائي الحاد واحتمال المجاعة في غزة. بالتوازي مع هذه التقارير، ظهرت عدة موضوعات إعلانية تُعارض أو تُعيد صياغة هذه السردية، بما في ذلك «حماس تسرق المساعدات» ورسائل تُؤكد أن «الرهائن» هم الضحايا الرئيسيون للحرمان («المساعدات تدخل غزة لكن الرهائن يتضورون جوعًا»). يُشير التزامن الزمني لهذه الموضوعات مع ذروة التقارير الإنسانية إلى استراتيجية إعلامية تفاعلية تهدف إلى صياغة التفسيرات والمُبررات للأزمة.

في المقابل، شهدت بعض الموضوعات حضورًا أكثر استدامة بمرور الوقت. فالحملات المستهدفة للمؤسسات والمنظمات الدولية – كتلك المُوّجهة ضد وكالة غوث وتشغيل اللاجئين الفلسطينيين - الأونروا، تقارير الأمم المتحدة، أو محكمة العدل الدولية - ظلت نشطة خلال معظم فترة الرصد، وإن كان ذلك بمستويات أقل من حيث الكثافة. وبالمثل، كذلك الموضوعات المرتبطة بالمؤسسات الحكومية (مثل حملات وزارة التربية والتعليم، وزارة النقل، أو التأمين الوطني) بقيت نشطة بنسبة ثابتة ومنخفضة لفترة مطوّلة، مما يدل على وجود طبقة خلفية من التواصل المؤسساتي بدلًا من تعبئة عرضية.

بالعموم، تكشف الأرقام عن بنية مزدوجة في الديناميكيات الزمنية للحملة. فمن جهة، تُستخدم موضوعات عالية التأثير بدفعات قصيرة ومُكثّفة مرتبطة بأحداث محددة أو أخبار يتداولها الإعلام. ومن جهة أخرى، تبقى مجموعة من المواضيع بدرجة أقل من الكثافة - والتي غالبًا ما تكون مؤسساتية أو تنتقد جهات دولية - حاضرة باستمرار.

تثير هذه الأنماط تساؤلات مهمة حول استخدام بنى الإعلانات الإلكترونية من أجل النشر الاستراتيجي لمعلومات قد تكون مُضللة أو جدلية. وبينما لا تصنف المنصة هذه الإعلانات على أنها سياسية، فإن المحتوى الموضوعاتي والاستهداف الزمني يشيران إلى إمكانية استخدام إعلانات جوجل ليس فقط للترويج، بل أيضًا لتشكيل وصياغة سرديات حول قضايا سياسية وإنسانية بالغة الحساسية. وعلى وجه الخصوص، فإن وجود التقارير الإنسانية حول انعدام الأمن الغذائي في غزة مع موضوعات إعلانية تُشكك في المسؤولية عن هذه الأوضاع أو تعيد تفسيرها أو تُعيد توجيه أصابع الاتهام لجهات مختلفة، يُشير إلى استخدام الإعلان كأداة للتدخل في السرديات. تستطيع هذه الحملات، عبر استغلال عرض الإعلانات المستهدفة والحساسة للتوقيت، أن تضخم تفسيرات محددة للأحداث.

4.3 تحليل نوعيّ لإعلان

لتوكيد النتائج الكميّة، يستعرض القسم التالي تحليلًا معمقًا لإعلان مُنتقى. ويُظهر كيف تُشكّل السرديات وكيف للتضليل الإعلامي أن يبرز من خلال تقنيات كالاقتباس الانتقائي، التجريد من السياق، والتأطير المُضلل.

قمنا بمعاينة أحد الأمثلة لإعلان موصوف تحت موضوع «ضد محكمة العدل الدولية». إليكم بالتالي نصّ الإعلان:

تعرّفوا على أحدث قضاة محكمة العدل الدولية
محمود ضيف الله حمود
«لا تملك إسرائيل حق الدفاع عن نفسها»
هذا كلامه
هذا ليس قاضٍ
بل إنه مُدعّي
وقد استبدل نواف سلّام
الذي وصف إسرائيل بالعدو
رحل قاضٍ معادٍ

وجاء آخر محله
في محكمة العدل الدولية، عدم الانحياز هو محض اقتراح
وليس مطلبًا
أمست محكمة العدل الدولية سيركًا سياسيًا
فقدت محكمة العدل الدولية شرعيّتها بالكامل

ظاهرياً، يُقدّم الإعلان نفسه على أنه نقدٌ واقعيّ لمحكمة العدل الدولية. إلا أن التدقيق فيه يكشف أن ادعاءاته تعتمد على اقتباسات انتقائية، وتجريد من السياق، وتأطير مُضلل.

أولًا، يُورد التصريح المُسند إلى محمود ضيف الله حمود («لا تملك إسرائيل حق الدفاع عن نفسها») من دون سياق. ووفقًا لتقرير لـ«ميدل ايست مونيتور»، ادعى حمود في حديثه لسفير الأردن بالأمم المتحدة، أن إسرائيل لا تملك أي حق في ادعاء الدفاع عن النفس في الأراضي المُحتلة كقطاع غزة، بموجب القانون الدوليّ. أعيد تأطير هذا الادعاء القانونيّ في الاعلان كأنه تصريح مُطلق وموقف مدفوع بنوايا سياسية، وعليه فهو يشوّه المعنى الأصلي.

بالمثل، الايحاء إلى نوّاف سلّام هو مُضلل بحد ذاته. يزعم الإعلان أنه «وصف إسرائيل بالعدو»، مما يوحي بانحياز لا يتوافق مع الحياد القضائي. إلا أنه يبدو أن هذا التصريح من تعليقات لسلّام كرئيس وزراء لبنان، حيث اعتبر إسرائيل «عدوًا» في سياق احتلال اسرائيل لأراضٍ لبنانية ونقاشات عن القرار الأممي 1701. كما أوردت «العربية»، فإن هذه التعليقات كانت جُزءًا من تصريحات سياسية أوسع معنية بتطبيق وقف اطلاق النار والانسحاب من الأراضي اللبنانية، وليس في تعبير عن انحياز قضائي. عبر تجريد هذا السياق، يبني الإعلان سردية العداء المنهجي من قبل المحكمة.

عبر هذه الأوصاف والتمثيل، يُشجع الإعلان مزعم أوسع بأن محكمة العدل الدولية منحازة بالفطرة وفاقدة للشرعية. هذا الاستنتاج غير مدعوم بالأدلة والبيّنات، بل هو ينبع كأثر متراكم للتجريد من السياق وتأطير التصريحات بشكل استراتيجي هادف. هذه التقنيات هي من سيم ممارسات التضليل الإعلامي، إذ لا يتم تزييف العناصر صراحة أو إختراعها من لا شيء، بل يجري التلاعب بها وتحريفها بطرق تضلل الجماهير إزاء معناها الحقيقي وعواقبها.

وعواقب هذه الرسائل بالذات وخيمة نظرًا لدور محكمة العدل الدولية كونها الهيئة القضائية الأعلى المنبثقة عن الأمم المتحدة. وقت سريان الحملة كانت المحكمة تتداول باجراءات تخص الاتهامات المعنية بانتهاكات القانون الدولي في غزة، يشمل ملف دعوى مرفوعة تحت ميثاق منع الإبادة الجماعية. في هذا السياق، من شأن الجهود الساعية لتقويض الحياد المنظور وشرعية المحكمة أن تُفهم كمحاولات لصياغة وتشكيل التصوّرات العامة حول الاجراءات القانونية الجارية.

وفقا لنطاق الانطباعات المُبلغ عنه من منصة الإعلان، عُرض هذا الإعلان ما بين 2,39 و 2,75 مليون مرة بالتقريب، مما يشير إلى مستوى عالٍ جدًا من الانكشاف. هذا الحجم من الانكشاف إنما يُشير إلى أن الرسالة لم تكن هامشية بل نُشرت على نطاق واسع، مما يزيد من احتمال تأثيرها على التصورّات العامة. في سياق التحليل

السابق، يعزز هذا المستوى من الوصول الحجة القائلة بأن إعلانات جوجل يمكن أن تكون وسيلة فعالة لنشر التضليل الإعلامي، لا سيما عند استخدامها بطريقة مُستهدفة حساسة للتوقيت.

مُباحثة

سعت هذه الورقة البحثية لمُعاينة كيفية توظيف منصة إعلانات جوجل كأداة في التأثير المعلوماتيّ، ومُعاينة خصائص ومحتوى هذه الحملات. توّفر النتائج عدة رؤىً قيّمة حول كلٍّ من التوظيف الاستراتيجي للإعلانات وآثاره على التضليل الإعلامي المُعاصر.

أولًا، تُشير الأنماط الزمنية المُعاينة في البيانات إلى أن العديد من الحملات الإعلانية لا تُنفّذ بشكلٍ مُستمر ومُتواصل، بل تُفعّل على شكل دفعات قصيرة ومُركّزة تتزامن مع أحداث مُحدّدة. تُظهر مواضيع مثل «تصويت اليوروفيجن» أو السرديات المعنية بانعدام الأمن الغذائي في غزة نقاط ذروة واضحة وبارزة تتزامن مع لحظات ازدياد اهتمام الجمهور. تُجيب هذه النتيجة بشكلٍ مُباشر على سؤال البحث الأول، وتتفق مع نظريات تأثير المعلومات التي تُؤكّد على التوقيت والأهمية، حيث تتدخّل الجهات الفاعلة تحديدًا عندما يبحث الجمهور بشكل نشط عن المعلومات، وبالتالي يكون أكثر عُرضةً لتأثيرات التأطير [45، 23]. بالإضافة إلى هذه القفزات قصيرة الأجل، تُظهر موضوعات أخرى - مثل تلك التي تستهدف وكالة غوث وتشغيل اللاجئين الفلسطينيين (الأونروا) أو مؤسسة هند رجب - نشاطًا أكثر استدامة على مدى فترات أطول، مما يُشير إلى استراتيجية مُكمّلة لتعزيز السردية بشكلٍ مُستمر.

ثانيًا، في سياق الإجابة على سؤال البحث الثاني، يكشف التوزيع الجغرافي للإعلانات عن استراتيجية استهداف واسعة النطاق ومتعددة البلدان في جميع أنحاء أوروبا. فبدلًا من التركيز على جمهور وطني واحد، تم نشر الحملات في مناطق متعددة في وقت واحد، مما يشير إلى محاولة لصياغة الرأي العام الدولي. ويتماشى هذا الاستهداف العابر للحدود مع منطق الدعاية الإعلامية واستراتيجيات الاتصال والإعلام الخارجي الساعية للتأثير على عموم الجماهير الأجنبية [8، 39]. كما يعكس أيضًا إمكانيات أنظمة الإعلان الرقمي، التي تُمكّن من الاستهداف الجغرافي الدقيق واسع النطاق.

ثالثًا، يُظهر تحليل بيانات الانطباعات (مرات العرض) أن الانكشاف أو التعرض يتركز بموضوعات مُعينّة بالذات، ويصل إلى جماهير واسعة جدًا، حيث تُعرض بعض الإعلانات ملايين المرات. يتوافق هذا الظهور المُركز مع منطق المزاد في إعلانات جوجل، حيث تُمكّن الميزانيات المرصودة واستراتيجيات المُزايدة الجهات الفاعلة من تضخيم رسائل محددة على نطاق واسع [6، 32]. في الوقت نفسه، تكشف البيانات عن أنماط تكرار عالية التردد، إما من خلال دفعات قصيرة من الانكشاف المُكثف، أو من خلال تكرار مستمر أقل كثافة على مدى فترات أطول. هذه الديناميكيات مهمة بشكل خاص في ضوء أثر وهم الحقيقة، حيث يؤدي الإنكشاف المُتكرر إلى زيادة المصداقية المُتصوّرة [37، 5]. بهذا المعنى، لا تصل الحملات الإعلانية إلى جماهير واسعة فحسب، بل تعرض السرديات ذاتها بشكل متكرر على

المستخدمين أيضًا، مما يعزز تأثيرها المُحتمل.

رابعًا، يُقدّم التحليل النوعي نظرةً ثاقبةً على محتوى هذه الإعلانات وبنيتها. يُبيّن المثال المدروس كيف يُمكن إنتاج المعلومات المُضلّلة ليس عن طريق التلفيق الصريح، بل من خلال الاقتباس الانتقائي، وإخراج المعلومات من سياقها، والتأطير المُضلّل.

تُستخرج التصريحات من سياقها القانوني أو السياسي الأصلي، ويُعاد تجميعها في سردية تُشكّك في شرعية المؤسسات الدولية مثل محكمة العدل الدولية. يتوافق هذا مع ما تُسمّيه الأدبيات بالمعلومات المُضلّلة أو المحتوى المُضلّل، والذي يصعب تنظيمه بشكل خاص لأنه يعتمد على معلومات دقيقة جزئيًا [73]. تُجيب هذه النتائج مباشرةً على سؤال البحث الثالث من خلال توضيح كيفية بناء السرديات وكيف يتم تشكيل المعنى استراتيجيًا.

تشير هذه النتائج مجتمعةً إلى أن إعلانات جوجل يمكن أن تؤدي دور أداة هجينة للدبلوماسية العامة والتضليل. فحتى إن توافقت مع سياسات المنصة - لا سيما بسبب التعريف الضيق للإعلانات السياسية المتعلقة بالانتخابات - فإن الحملات التي قمنا بتحليلها هنا تنشط في المساحة الضبابية من التواصل القائم على القضايا. وهذا يُبرز فجوة بين أطر حوكمة المنصات والتأثير المعلوماتي الأوسع لمثل هذا المحتوى، وقدرته على نشر سرديات مهمة سياسيًا على نطاق واسع دون أن تؤدي إلى تنظيم أكثر صرامة [34، 33].

وبالعموم، تُوسّع هذه الدراسة نطاق الأبحاث الحالية حول التضليل الإعلامي، والتي ركزت بشكل أساسي على التلاعب والتحريف عبر وسائل التواصل الاجتماعي والسلوك غير الأصيل المنسق [14]. وتُظهر أن بنى الإعلانات المدفوعة تُشكّل قناة إضافية للتأثير والتي لم تُدرس بشكلٍ كافٍ. بعكس المحتوى العضوي، يسمح إعلان البحث للجهات الفاعلة بإدراج الرسائل مباشرةً في لحظات البحث عن المعلومات، حيث يكون المستخدمون أكثر ميلًا للوثوق بالمعلومات التي يصادفونها والاعتماد عليها [55، 26]. وهذا يخلق ظروفًا يمكن في ظلها أن يؤثر التعرض الأولي على التفسير اللاحق، معززًا استمرار السرديات المُضللة حتى بوجود معلومات تصحيحية [45].

خُلاصة

تناولت هذه المقالة كيفية استخدام بنية إعلانات جوجل التحتية كأداة للتأثير المعلوماتي المرتبط بالدولة، وذلك من خلال دراسة الحملات الحكومية الإسرائيلية. وبدمج التحليل الكمي لبيانات الإعلانات مع الفحص النوعي لمُحتواها، تُظهر الدراسة كيف تُتيح أنظمة الإعلان الرقمي النشر على نطاق واسع والتأطير الاستراتيجي للسرديات ذات الحساسية السياسية.

وتُبين النتائج أن هذه الحملات تتميز بالنشر الزمني المُستهدف، والانتشار الجغرافي العابر للحدود، والانكشاف (التعرض) المُركز للغاية، حيث تصل غالبًا إلى ملايين المستخدمين.

كما تُبين كيف يُمكن لمحتوى الإعلانات الاعتماد على تقنيات مرتبطة بالتضليل الإعلامي، بما في ذلك التأطير الانتقائي والتجريد من السياق، لتشكيل تفسيرات القضايا الجدلية.

لهذه النتائج عدة دلالات. أولًا، تُشير إلى ضرورة أن يتجاوز البحث في مجال التضليل الإعلامي التركيز الضيق على وسائل التواصل الاجتماعي، وأن يُدمج دور أنظمة البحث والإعلان كبنى تحتية رئيسية للظهور والتأثير. ثانيًا، تُشير النتائج إلى وجود قصور في حوكمة المنصات الحالية، ولا سيما التمييز بين الإعلانات الانتخابية ذات الطابع السياسي والتواصل الأوسع نطاقًا القائم على القضايا. ثالثًا، تُبرز هذه الدراسة أهمية أدوات الشفافية أمثال مركز شفافية الإعلانات من جوجل، مع الكشف في الوقت نفسه عن محدودياتها، بما في ذلك التأخير في إعداد التقارير والبيانات غير المكتملة.

إجمالًا، تُسهم هذه الدراسة في مجموعة متنامية من الأبحاث حول بيئات المعلومات الرقمية من خلال إظهار أن الإعلان ليس مجرد أداة تجارية، بل هو أيضًا أداة قوية للتأثير المعلوماتي. وبذلك، فإنها تُثير تساؤلات أوسع نطاقًا حول مسؤولية المنصات، والمساءلة الديمقراطية، وتنظيم الظهور في المجال العام الرقمي.

المراجع

1. Waqas Ahmad et al. Companies inadvertently fund online misinformation through advertising.
2. Nature, 2024. Evidence on advertising financing of misinformation supply chains.
3. Al Jazeera Centre for Studies. Digital occupation: Pixelated propaganda, censored platforms, and the battle for narrative in gaza, 2024. Accessed 202512-12-.
4. Al Jazeera Media Institute. Information warfare and the battle over gaza's narrative, 2024. Accessed 202512-12-.
5. Al-Shabaka: The Palestinian Policy Network. Israel's disinformation apparatus: A key weapon in its arsenal, 2022. Accessed 202512-12-.
6. Gordon W. Allport and Leo Lepkin. Wartime rumors of waste and special privilege: Why some people believe them. Journal of Abnormal and Social Psychology, 40(1):3–36, 1945.
7. Alphabet Inc. Form 10-k for fiscal year ended december 31, 2024 (sec filing). https://ww w.sec. gov/Archives/edgar/data/165204400016520442500001 4//goog-20241231.htm, February 2025. Business description and revenue discussion for Google Services advertising.
8. Amnesty International. Amnesty international report on genocide in gaza. https://web.ar chive. org/web/20250724065956/https://amnesty.ca/wp-content/uploads/202412//Am nesty-International-Gaza-Genocide-Report-December-42024-.pdf, December 2024.
9. Miriyam Aouragh. Hasbara 2.0: Israel's public diplomacy in the digital age. Middle East Critique, 25(3):271–297, 2016.
10. David S Ardia, Evan Ringel, Victoria Ekstrand, and Ashley Fox. Addressing the decline of local news, rise of platforms, and spread of mis-and disinformation online: A summary of current research and policy proposals. UNC Legal Studies Research Paper, 2020.
11. William Audureau, Samuel Forey, and Assma Maad. "quarante b´eb´es d´ecapit´es": itin´eraire d'une rumeur au cœur de la bataille de l'information entre isra¨el et le hamas, April 2024. Accessed 202512-12-.
12. L´ıvia Benkov´a. The rise of russian disinformation in europe. Austria Institut fu¨r Europa und Sicherheitspolitik, 2018.
13. Jonah Berger. Arousal increases social transmission of information. Psychological science, 22(7):891–893, 2011.
14. Samantha Bradshaw and Philip N. Howard. The global disinformation order: 2019 global inventory of organised social media manipulation. Technical report, Oxford Internet Institute, 2019. Accessed 202516-12-.
15. Samantha Bradshaw and Philip N. Howard. Industrialized disinformation 2020 global inventory of organized social media manipulation. Technical report, Oxford Internet Institute, University of Oxford, 2020. Accessed 202517-12-.
16. Michal- Chora´s, Konstantinos Demestichas, Agata Giel-czyk, A´lvaro Herrero, Pawel- Ksieniewicz, Konstantina Remoundou, Daniel Urda, and Michal- Wo´zniak. Advanced machine learning tech-niques for fake news (online disinformation) detection: A systematic mapping study. Applied Soft Computing, 101:107050, 2021.
17. Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, and Michele Starnini. The echo chamber effect on social media. Proceedings of the National Academy of Sciences of the United States of America, 118(9):e2023301118, 2021. Accessed 202512-12-.
18. Ellen M Cotter. Influence of emotional content and perceived relevance on spread of urban legends: A pilot study. Psychological reports, 102(2):623–629, 2008.
19. The Cradle. Cyprus: Netanyahu's new haifa. The Cradle, 2025.
20. La Croix. Loin de la ¨terre promise¨et de la guerre, ces isra´eliens qui s'installent en gr`ece. La Croix International, 2025.
21. Nicholas John Cull. Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present. ABC-CLIO, 2003.
22. Carlos A. D´ıaz Ruiz et al. Disinformation and fake news as externalities of digital advertising markets. Journal of Marketing Management, 2024. Discusses how advertising market incentives can sustain harmful information ecosystems.

23. Drop Site News. Google's $45 million contract with netanyahu's office to spread israeli pro-paganda. https://www.dropsitenews.com/p/google-youtube-netanyahu-israel-propaganda-gaza-famine, September 2025.
24. Ullrich K. H. Ecker, Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. The psychological drivers of misinformation belief and its resistance to correction. Nature Reviews Psychology, 1:13–29, 2022.
25. Allen L Edwards. The relationship between the judged desirability of a trait and the probability that the trait will be endorsed. Journal of applied Psychology, 37(2):90, 1953.
26. Allen L Edwards. The social desirability variable in personality assessment and research.
27. Dryden Press, 1957.
28. Robert Epstein and Ronald E. Robertson. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proceedings of the National Academy of Sciences, 112(33):E4512–E4521, 2015.
29. European External Action Service. Euvsdisinfo, 2023. Accessed 202512-12-.
30. European External Action Service. Second eeas report on foreign information manipulation and interference threats. Technical report, EEAS, 2023. Accessed 202516-12-.
31. Jean-Pierre Filiu. Anatomy of an israeli disinformation campaign, July 2024. Accessed 202512-12-.
32. Richard Fletcher, Alessio Cornia, Lucas Graves, and Rasmus Kleis Nielsen. Measuring the reach of" fake news" and online disinformation in europe. Australasian Policing, 10(2):25–33, 2018.
33. Nathaniel Gleicher. Removing coordinated inauthentic behavior from israel, 05 2019. Accessed 202517-12-.
34. Google. How the google ads auction works / ad rank. https://support.google.com/google-ads/answer/6366577?hl=en, 2025. Documentation describing auction-based placement and Ad Rank factors.
35. Google. Misrepresentation — advertising policies help. https://support.google.com/ads policy/answer/6020955?hl=en, 2025.
36. Google. Political content — advertising policies help. https://support.google.com/adspo licy/answer/6014595?hl=en, 2025.
37. Google Business. Ai-powered search marketing. https://business.google.com/us/think
38. /search-and-video/ai-powered-search-marketing/, 2025. Accessed 202517-12-.
39. Andrew M Guess and Benjamin A Lyons. Misinformation, disinformation, and online propa-ganda. Social media and democracy: The state of the field, prospects for reform, 10:10–33, 2020.
40. Lynn Hasher, David Goldstein, and Thomas Toppino. Frequency and the conference of referential validity. Journal of Verbal Learning and Verbal Behavior, 16(1):107–112, 1977.
41. Chip Heath, Chris Bell, and Emily Sternberg. Emotional selection in memes: the case of urban legends. Journal of personality and social psychology, 81(6):1028, 2001.
42. Bernd Hirschberger. External Communication in Social Media During Asymmetric Conflicts. transcript Verlag, 2021.
43. Simon Hooper and Dania Akkad. Israel–palestine war: How unverified reports of hamas 'beheading babies' filled front pages, October 2023. Accessed 202512-12-.
44. i24NEWS. 'it smells of death' here — surveying the scenes of atrocities in kfar aza, 2023. Accessed 202512-12-.
45. Institute for Middle East Understanding. Fact sheet: Israel's history of spreading disinforma-tion, 2023. Accessed 202512-12-.
46. Alexander Lanoszka. Disinformation in international politics. European journal of interna-tional security, 4(2):227–248, 2019.
47. David MJ Lazer, Matthew A Baum, Yochai Benkler, Adam J Berinsky, Kelly M Greenhill, Filippo Menczer, Miriam J Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, et al. The science of fake news. Science, 359(6380):1094–1096, 2018.
48. Stephan Lewandowsky, Ullrich K. H. Ecker, and John Cook. Misinformation and its correction: Continued influence and successful debiasing. Psychological Science in the Public Interest, 13(3):106–131, 2012. Accessed 202512-12-.
49. Volodymyr Lysenko and Catherine Brooks. Russian information troops,

disinformation, and democracy. First Monday, 2018.

50. Diego A Martin, Jacob N Shapiro, and Michelle Nedashkovskaya. Recent trends in online foreign influence efforts. Journal of Information Warfare, 18(3):15–48, 2019.
51. Alice Marwick and Rebecca Lewis. Media manipulation and disinformation online. New York: Data & Society Research Institute, 359:1146–1151, 2017.
52. Timothy P McGeehan. Countering russian disinformation. The US Army War College Quar-terly: Parameters, 48(1):7, 2018.
53. Dana¨e Metaxa-Kakavouli and Nicol´as Torres-Echeverry. Google's role in spreading fake news and misinformation. Technical report, SSRN, October 2017. Available at SSRN: https://ssrn.com/abstract=3062984.
54. Susan Morgan. Fake news, disinformation, manipulation and online tactics to undermine democracy. Journal of cyber policy, 3(1):39–43, 2018.
55. Bennet B. Murdock. The serial position effect of free recall. Journal of Experimental Psychol-ogy, 64(5):482–488, 1962.
56. Raymond S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, 2(2):175–220, 1998.
57. Organisation for Economic Co-operation and Development. Facts not fakes: Tackling disinfor-mation, strengthening information integrity. Technical report, OECD, Paris, 2024. Accessed 202516-12-.
58. Bing Pan, Helene Hembrooke, Thorsten Joachims, Lori Lorigo, Geri Gay, and Laura Granka. In Google we trust: Users' decisions on rank, position, and relevance. Journal of Computer-Mediated Communication, 12(3):801–823, 2007.
59. Christopher Paul and Miriam Matthews. The russian "firehose of falsehood" propaganda model. Technical report, RAND Corporation, 2016. Accessed 202516-12-.
60. Andrea Pereira, Elizabeth Harris, and Jay J. Van Bavel. Identity concerns drive belief: The impact of partisan identity on the belief and dissemination of true and false news. Group Processes & Intergroup Relations, 26(1):24–47, 2023.
61. Kim Peters, Yoshihisa Kashima, and Anna Clark. Talking about others: Emotionality and the dissemination of social information. European Journal of Social Psychology, 39(2):207–222, 2009.
62. The Jerusalem Post. Trilateral work plan for military cooperation between israel, greece, cyprus signed - exclusive. The Jerusalem Post, 2025.
63. Kristen Purcell, Joanna Brenner, and Lee Rainie. Search engine use 2012. Technical report, Pew Research Center, March 2012. Report and topline findings on U.S. search engine use and preferences.
64. Edward W. Said. Propaganda and war. Media Monitors Network, August 2001.
65. Simona Stano et al. The internet and the spread of conspiracy content. In Routledge handbook of conspiracy theories, pages 483–496. Routledge, 2020.
66. Charles S. Taber and Milton Lodge. Motivated skepticism in the evaluation of political beliefs.
67. American Journal of Political Science, 50(3):755–769, 2006.
68. The New Arab. Israel to quadruple hasbara spending in bid to salvage global reputation, 2024. Accessed 202517-12-.
69. The Washington Post. Google email shows it ruled israel's ads claiming 'there is food in gaza' aren't misleading. https://www.washingtonpost.com/technology/202515/10//israel-ads-youtube-famine-gaza/, October 2025. Reports on policy complaints and Google's decision regarding Israel-promoted ads about Gaza famine claims.
70. Craig Timberg and Tony Romm. Facebook shuts down israel-based disinformation campaigns as election manipulation increasingly goes global. The Washington Post, May 2019. Accessed 202517-12-.
71. Kathie M d'I Treen, Hywel TP Williams, and Saffron J O'Neill. Online misinformation about climate change. Wiley Interdisciplinary Reviews: Climate Change, 11(5):e665, 2020.
72. TRT World. How israel uses disinformation to shape the gaza narrative, 2024. Accessed 202512-12-.
73. TRT World. Israel pumps millions into a disinformation campaign to deny gaza famine.
74. https://www.trtworld.com/article/26aa3a47f85b, September 2025.
75. United Nations Office for the Coordination of Humanitarian Affairs and Office of the High Commissioner for Human

Rights. Special rapporteur report on gaza: Genocide as a collective crime, October 2025. Accessed 202512-12-.

76. Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi. The spreading of misinformation online. Proceedings of the National Academy of Sciences, 113(3):554–559, 2016.
77. Nathan Walter and Riva Tukachinsky. A meta-analytic examination of the continued influence of misinformation in the face of correction: How powerful is it, why does it happen, and how to stop it? Communication research, 47(2):155–177, 2020.
78. Claire Wardle and Hossein Derakhshan. Information disorder: Toward an interdisciplinary framework for research and policymaking. Technical Report 27, Council of Europe, 2017.
79. Jen Weedon, William Nuland, and Alex Stamos. Information operations and facebook, 2017.
80. WIRED. Israel is buying google ads to discredit the UN's top gaza aid agency. https:
81. //www.wired.com/story/israel-unrwa-usa-hamas-google-search-ads/, August 2024. Reports on Israel-linked Google Search ads targeting UNRWA/UNRWA USA queries.

الذكاء الاصطناعي في النظام الإنساني بغزة: **تأمل نسوي استعماري عن السيطرة والوصول**

روان يوسف

روان عالمة سياسة؛ نسوية وباحثة حول الاستعمار. حاصلة على ماجستير في دراسات التنمية من جامعة إيراسموس، وهي حاليًا مرشحة دكتوراه في العلوم السياسية في الجامعة العبرية بالقدس. يجسر عملها بين النظرية النسوية والعمل الإنساني والنقد منهاضٍ للاستعمار، مع سجل قوي في البحث الميداني والإرشاد الأكاديمي.

تبحث روان في كيفية تشكيل الأنظمة الإنسانية المعتمدة على الذكاء الاصطناعي لعمليات إيصال المساعدات في غزة والضفة الغربية والقدس الشرقية. ومن خلال عدسة نسوية مناهضة للاستعمار، تحلل كيف تُدرِج الأدوات الرقمية - مثل التسجيل البيومتري والخوارزميات التنبؤية - آليات المراقبة وتعيد إنتاج عدم المساواة البنيوية.

إجازة

تبحث هذه الورقة في كيفية عمل الذكاء الاصطناعي والأنظمة الرقمية الأوسع في قطاع العمل الإنساني ذي العلاقة بغزة، تحت ظروف الحصار وتدمير البنية التحتية والتجسس والسيطرة الخارجية. بدلًا من التعامل مع الذكاء الاصطناعي على أنه ابتكار مُتميّز، تقدّم الدراسة تحليلًا يتناول كيف يواجه العاملين في الإغاثة الانسانية الأنظمة المرتبطة بالذكاء الاصطناعي والأنظمة الرقمية، وكيف يتعاملون معها ويفسرونها في ممارستهم اليومية. بالاعتماد على عشر مقابلات نوعية مع عاملين في قطاع الاغاثة الانسانية من الفلسطينيين وغير الفلسطينيين، تُبيّن الورقة البحثية هذه أن الذكاء الاصطناعي يظهر في شكلين متشابكين: استخدام الموظفين غير الرسمي للأدوات التوليدية للتعامل مع الضغط الإداري، والأنظمة الرقمية المؤسساتية التي تنظم التسجيل، التحقق، الاستحقاق، الإبلاغ، وتداول البيانات الإنسانية.

تجادل الورقة بأن أهمية الذكاء الاصطناعي التقنية في غزة أقل من أهميته المؤسساتية. تعمل الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي كبنى تحتية للحوكمة الإنسانية وتكثف التصنيف، توّسع تداول البيانات من دون رقابة، وتعيد توزيع العمل، المخاطر، والسُلطة عبر سلسلة عملياتية غير متكافئة. تكشف النتائج عن أربع ديناميكيات متكررة: التبني غير الرسمي للذكاء الاصطناعي في ظل حوكمة ضعيفة، السيطرة الخارجية على الفئات والقوائم، تحويل العمل والمخاطر إلى أسفل السلسلة القيادية، والتعامل اليومي في ظل ظروف الرعاية والتعرض والمسؤولية المُقيّدة.

من خلال الجمع بين المنح الدراسية حول الحوكمة الإنسانية والبيانات الهامة ودراسات الذكاء الاصطناعي والحكم الاستعماري الاستيطاني والاقتصاد السياسي النسوي، تعيد الورقة صياغة الذكاء الاصطناعي في العمل الإنساني بعيدًا عن قوائم المخزون القائم، قوائم مراجعة الأخلاقيات، باتجاه الحوكمة في حيّز الإغاثة الانسانية القائم تحت الاستعمار. ويظهر أنه في غزة، يكثف الذكاء الاصطناعي علاقات الهيمنة البيروقراطية القائمة، التبعية المعرفية، والمنافسة المُقيَّدة.

كلمات مفتاحية: **الذكاء الاصطناعي؛ حوكمة الإغاثة الانسانية؛ المساعدات الرقمية؛ غزة**

توطئة

تتم مناقشة الذكاء الاصطناعي بشكل متزايد على أنه يعيد تشكيل حوكمة الاغاثة الانسانية، إلا أنه يدخل من خلال الأطر المؤسساتية الرسمية في العديد من البيئات العملياتية بشكل غير متساوٍ وغير رسميّ وجزئيّ فقط. في غزة، تبدو الأنظمة ذات العلاقة بالذكاء الاصطناعي والمنظومات الرقمية كابتكارات تنظيمية بدرجة أدنى من الوضوح، بل تبدو إلى حدٍ كبير جزءًا من الممارسة الإدارية اليومية، التي تتم من خلال منصات واجراءات صُممت في مواقع أخرى، على أن يجري العمل عليها والتنقل بين مختلف المنصات والاجراءات تحت قيود سياسية وعملياتية مُشددة.

وعليه، لكي نتمكن من فهم دورها، واجب علينا أن نُشيح بتركيزنا من التصميم المؤسساتي إلى الحوكمة كما تُختبر في المُمارسة العملية.

تقدم غزة حالة كاشفة بشكل خاص. تجري أعمال الاغاثة الإنسانية في بيئة مُقيّدة للغاية بفعل الحصار، العنف المتكرر واسع النطاق، السلطة المُجزّأة والمُشرذمة، وإتاحة الوصول للبنى التحتية والسلع والأنظمة المالية بوساطة خارجية. يعتمد التنسيق وتقديم المساعدة والتحقق من الأهلية والاستحقاق بشكل متزايد على المنصات الرقمية وترتيبات الإدارة عن بُعد وإجراءات البيانات الموحدة المعيارية. تتضمن بعض هذه العمليات أدوات مدعومة بالذكاء الاصطناعي، بينما يعكس العديد منها أشكالًا أوسع من الرقمنة. لذلك فإن التمييز بين الذكاء الاصطناعي والحوكمة الرقمية ضروري على المستوى التحليلي.

في هذه الورقة، تشير «الأنظمة ذات العلاقة بالذكاء الاصطناعي» إلى الأدوات التي تتضمن المعالجة الخوارزمية أو دعم القرار الآلي أو أدوات الذكاء الاصطناعي التوليدية. يُقصد بـ»الأنظمة الرقمية» بالعموم، أدوات التنسيق القائمة على المنصة، البنى التحتية للتسجيل، قواعد البيانات، والتقنيات الإدارية التي تشكل مبنى الإغاثة والعمل الإنساني دون الاعتماد بالضرورة على الذكاء الاصطناعي. لا تعتمد جميع أشكال الحوكمة الرقمية المعنية بالعمل الإنساني في غزة على الذكاء الاصطناعي، حتى حينما تشكل أشكال الوصول والتصنيف والتنسيق والسيطرة. لذلك تُعاين الورقة البحثية الذكاء الاصطناعي في إطار مجال الحوكمة الرقمية الأوسع، وتبقى متيقظة لمحدوديات الأدلة المتاحة إزاء نشر الذكاء الاصطناعي رسميًا.

ترى الورقة البحثية أن الأنظمة ذات العلاقة بالذكاء الاصطناعي والأنظمة الرقمية في غزة تعمل كأدوات تكنولوجية منفصلة بقدر ما تعمل كبنى تحتية لحوكمة العمل الإنساني والإغاثة في غزة. وعوضًا عن مسح التبني المؤسساتي عبر قطاع العمل الإنساني والإغاثة، يُعاين البحث كيف يواجه العاملون في الإغاثة والعمل الانساني هذه الأنظمة، يفسرونها ويُديرون أعمالهم اليومية بين رحابها. في الاغاثة والعمل الإنساني المعنيّ بغزة، لا يُعدّ الذكاء الاصطناعي في المقام الأول تطورًا تكنولوجيًا، بل إنه آلية حوكمة تُعيد تنظيم الوضوح والقابلية، التشغيل، والسلطة في ظل ظروف القيود الاستعمارية. ويحوّل هذا الأمر الانتباه من سرديات الابتكار والحداثة المؤسساتية إلى الحوكمة المُجازة من خلال واجهات المستخدم، الإجراءات، الروتين المفوض، وسلاسل القرار الغامضة.

تساهم الورقة في الجدل والنقاشات الدائرة عن الذكاء الاصطناعي ذي الطابع الإنساني والحوكمة الرقمية من خلال إبراز الممارسة اليومية في سياق سياسي شديد التقييد. الدراسات البحثية القائمة في الأدبيات، سبق أن درست الحوكمة الخوارزمية، الإغاثة الإنسانية القائمة على البيانات، والاقتصاد السياسي لأنظمة المساعدات الرقمية، لكنها غالبًا ما ركّزت على الاستراتيجية التنظيمية أو التصميم التكنولوجي أو آثار السياسات واسعة النطاق، عوضًا عن التركيز على كيف يتم ترتيب وتسوية الأنظمة في الممارسة العملية. بالتركيز على غزة، تُظهر هذه الدراسة أن الحوكمة المعتمدة على الذكاء الاصطناعي والحوكمة الرقمية لا تتم بالتحوّل المُؤسساتي الرسمي وحده، بل إنها تُسوّى وتُعاش عبر الأعمال الإدارية، العمل التفسيري، إدارة المخاطر، والرؤية المؤسساتية غير المتكافئة، التي تجري بشكل يوميّ.

يسترشد التحليل بثلاثة أسئلة بحثية: كيف يتعامل الموظفون العاملون في قطاع المساعدات الإنسانية والإغاثة في غزة مع الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي ويتنقلون فيما بينها؟ ما هي الآليات المؤسساتية والتقنية التي توظفها هذه الأجهزة لتنسيق الشؤون الإنسانية، اتخاذ القرارات، وتقديم المساعدات؟ كيف تفسر الجهات الفاعلة في الإغاثة والمساعدات الإنسانية الحوكمة المعتمدة على الذكاء الاصطناعي، تُسوّيها، وتطعن فيها، في ظل ظروف مرهونة بقيود سياسية وعملياتية؟

للنظر في هذه الأسئلة، تعتمد الورقة البحثية على مقابلات نوعية أجريناها مع العاملين في قطاع الإغاثة والمساعدات الإنسانية الناشطين في قطاع غزة عبر المنظمات الدولية والمحلية، مع استكمالها بالتحليل السياقي للمواد المعنية بالسياسات والمواد المؤسساتية. تظهر النتائج أن الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي تأخذ دور البُنى التحتية للحوكمة اليومية وهي مُدمجة بالروتين الإداري، بتبعيات المنصة، وبعمليات التحقق، بيد أن الجهات الفاعلة في الخطوط الأمامية تتعامل معها في ظروف من عدم اليقين، سيطرة تقنية غير متكافئة، ومخاطر سياسية مُتزايدة.

تتكوّن الورقة البحثية من خمسة أجزاء. يُحدد القسم التالي الإطار التحليلي، متبوعًا بمنهجية البحث. يستعرض فصل النتائج تحليلًا إمبيريًا تجريبيًا من خلال أربع ديناميكيات متكررة: التبني غير الرسمي في ظل الحوكمة الضعيفة، السيطرة الخارجية على الفئات والقوائم، تحويل العمل والمخاطر إلى أسفل السلسلة القيادية، والتعامل والتسوية اليوميّة في ظل ظروف الرعاية والتعرض والمسؤولية المُقيّدة. ويضع فصل المُباحثة هذه النتائج ضمن مناقشات أوسع معنية بحوكمة الإغاثة والعمل الإنساني وقوة التكنولوجيا، فيما يتناول فصل الخُلاصة آثارها الأوسع على السياسة.

الإطار التحليلي: الذكاء الاصطناعي بقطاع العمل الإنساني، الحوكمة الرقمية، والقوة الاستعمارية

تُظهر الأبحاث حول الذكاء الاصطناعي بقطاع العمل الإنساني والحوكمة الرقمية أن التقنيات المقدمة بلغة الكفاءة والابتكار غالبًا ما تعيد تنظيم السلطة والمساءلة بطرق أقل وضوحًا. تستطيع الأنظمة المدعومة بالذكاء الاصطناعي تضييق المساحة التفسيرية، تضمين الأحكام في البنى التحتية المُبهمة، وتعقيد الطعن في القرارات، في حين أن الأنظمة الرقمية تفضل التوحيد القياسي والمخرجات القابلة للقياس على الحكم السياقي (كوبي وآخرون، 2021 ؛ بوريل 2016؛ أناني وكروفورد 2018؛ ديفيدال 2024). عندما تكون الموافقة والرفض والاستعانة ضعيفة، فقد تضخم الأنظمة الضرر بدلًا من أن تخففه أو تقلله (بيدوشي 2022؛ لاتونيرو 2019؛ وايتزبرغ وآخرون، 2021). لذلك لا يتم التعامل مع الذكاء الاصطناعي هنا في المقام الأول كمجموعة أدوات بل كجزء من مجال أوسع للحوكمة الرقمية الذي يعمد إلى صياغة وتشكيل عمليات التصنيف والتحقق وصنع القرار.

ولا بُد من موضعته في السياق السياسي والمادي المحدد لغزة. تنشط أعمال الإغاثة والمساعدات الإنسانية هناك تحت الحصار، الاحتلال، تدمير البنية التحتية، تقييد الحركة، سلطة مُجزأة، والوصول للسلع والحاجيات والبنية التحتية والأنظمة المالية بوساطة خارجية. لا تدخل الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء

الاصطناعي حيزًا إداريًا محايدًا. بل هي تعمل ضمن بنية قائمة من التجسس، التوثيق، التصنيف، والمسؤولية المؤسساتية المُقيّدة. وبالتالي، فإن السؤال ليس فقط ما إذا كان الذكاء الاصطناعي يُستخدم، بل كيف تتم مواجهة الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي ضمن نظام أوسع لحوكمة الإغاثة والمساعدات الإنسانية في ظل القيود الاستعمارية.

وتساعد الأدبيات والدراسات في مجال حوكمة الإغاثة والمساعدات الإنسانية والحوكمة البيروقراطية على توضيح ذلك. يجري العمل على المساعدات بشكل متزايد بواسطة الإدارة عن بعد، الفئات المعيارية المُوّحدة، الإبلاغ الرقمي، والإدارة القائمة على القواعد بدلاً من المُحاسبة المباشرة (دونيني وامكسويل 2013؛ دافيلد 2007). ببساطة، لا تشخّص أنظمة التسجيل والتحقق الحاجة. بل إن تبني هذه الأنظمة مستفيدين شرعيين وينتج عنها إقصاء بعض الجهات حيث لا تتوافق حيوات البشر مع القوالب الإدارية (جاكوبسن 2015). لذلك يجب فهم النظم التكنولوجية ضمن الممارسة البيروقراطية العادية، إذ أن التنسيق، الاستحقاق والأهلية، التحقق، وتسليم المساعدات قد يبدو شأنًا تقنيًا فحسب، إلا أنه تترّتب عليه آثار توزيعية وسياسية.

كما تُظهردراسات البيانات والذكاء الاصطناعي المُهمّة جدًا كيف تُعيد هذه الأنظمة إنتاج القوة غير المُتكافئة من خلال البنى التحتية، الفئات المُحددة، والسلطة المعرفية. لا تنبع الضبابية الخوارزمية من شدة التعقيد التقني فحسب، بل من الترتيبات المؤسساتية المعنية بالبيانات ونماذج الذكاء الاصطناعي (بورل 2016؛ أناني وكراوفورد 2018). يصف كولدري وميجاس (2019 أ؛ 2019 ب) استخراج البيانات المعاصر بأنه تشكيل استعماري، بينما يوضح بيرهان (2020) كيف تعتمد أنظمة الذكاء الاصطناعي في الشمال العالمي على الممارسات الاستخراجية والمنطق التصنيفي المفروض الذي يُعيد إنتاج التبعية بدلاً من المسؤولية المحلية. في غزة، حيث لا تتحكم الجهات الفاعلة المحلية في البنى التحتية، مسارات البيانات، أو المعايير، تُعيد الأنظمة التقنية تنظيم الوضوح والقابلية، صنع القرار، والوصول، حتى حينما يفتقد الخاضعون لها لآليات شفافية إزاء كيفية عملها.

توّفر أبحاث الاستعمار الاستيطاني والحوكمة الاستيطانية الاستعمارية هيكل سياسي أوسع، يستوجب قراءة ودراسة هذه الأنظمة من خلاله. يؤطر وولف (2006) الاستعمار الاستيطاني كمبنى هيكلي متواصل للتصفية، الاحتواء والإدارة؛ بينما يوضح فيلدمان (2008) كيف أن غزة تُحكم من فترة طويلة بواسطة وثائق، تصاريح، فئات، وعدم اليقين الإداري. ويُضيف سعيد (1978) أن السلطة لا تعتمد فقط على الإكراه وإنما على المؤسسات التي تحدد ما هو معروف وقابل للحكم. وبالتالي، لا يجوز التعامل مع التسجيل، التحقق، التصنيف، والتنسيق في غزة كإجراءات محايدة. فهي متضمنة في علاقات الهيمنة البيروقراطية القائمة مُسبقًا والتي تتحكم بالتنقل، بالقابلية والوضوح، والوصول.

يحمل هذا الأمر أهمية خاصة نظرًا لعمل البنى التحتية الرقمية للإغاثة والأعمال الإنسانية في عصرنا تحت ظروف تتقاطع فيها رقابة الجهات المانحة، المزوّدين من القطاع الخاص، والمنطق الأمني بشكل متزايد. بدأت الأدبيات القانونية والسياساتية بإدراك الأهمية السياسية للبيانات المدنية في النزاعات المُسلّحة، مُحذّرة من بقاء مجال حماية البيانات متخلفًا على الرغم من الاعتماد المتزايد

على الأنظمة الرقمية المُركّزة (اللجنة الدولية للصليب الأحمر 2021؛ جيس 2021). كما تُظهر الأبحاث حول حوكمة بيانات الإغاثة والأعمال الإنسانية تداول البيانات الشخصية المجموعة لأغراض توزيع وتقديم المساعدات داخل النظم الإيكولوجية الأوسع التي تشكلت بفعل المانحين، والمتعهدين، الدول والمخاوف الأمنية؛ علمًا أن تداولها يتم بشكل خاص في بيئة توّفر للسكان المتضررين وسائل محدودة للطعن (GPPi معهد السياسة العامة الدولي 2021، جروت 2025). في غزة، لا تقع البنى التحتية الرقمية للإغاثة والأعمال الإنسانية خارج البُنى والهياكل الأمنية. بل إنها تعمل في بيئة مُشبعة بها.

يضيف الاقتصاد السياسي النسوي طبقة أخيرة من خلال إظهار كيف تعمل أنظمة الحوكمة بإعادة توزيع العمل والتشغيل، المخاطر والمسؤولية بدلًا من مجرد زيادة النجاعة. يوضح فريجر (2016) ويوبانكس (2018) كيف تُحوّل الرعاية والتوزيع إلى محض إدارة فنية بينما تُنقل المحاسبة لتُحال على الذين يعانون من العواقب. في غزة، غالبًا ما تعيش النساء هذه الأعباء وتواجهها أثناء تقديمها الرعاية غير مدفوعة الأجر، سعيها للبقاء والحفاظ على الأسر، التوثيق، المتابعة، والتعامل المُتكرر مع أنظمة المساعدات تحت واقع من الحصار والنزوح. كما تُظهر دراسات البيانات من منظور نسوي أن أنظمة البيانات تُشفّر الافتراضات المعيارية إزاء الأسر والاستحقاق والتي من شأنها أن تسيء تشخيص أولئك الذين لا يتوافقون مع أي من الفئات المعيارية المُوّحدة أو أن تستبعدهم منها (دي ايجنازيو وكلاين 2020). وعليه، لا بُد من قراءة الحوكمة الرقمية في غزة ليس فقط كمسألة تكنولوجيا وسيطرة، بل كإعادة إنتاج اجتماعي، كمسألة معنية بالكرامة، وإعادة توزيع التشغيل والعمالة بشكل غير مُتكافئ.

ولتحقيق هذه الغاية، يقدم هذا الإطار ثلاثة مُقترحات. أولًا، تعمل الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي في غزة كبنى تحتية للحوكمة عوضًا عن كونها أدوات محايدة. ثانيًا، تنشط هذه الأنظمة في مساحة استعمارية تتشكل من الحصار والاحتلال والسيطرة البيروقراطية. ثالثًا، يتم التنقل والتوسط في هذه الأنظمة بالعمل اليومي، التفسير، والأشكال غير المتكافئة من التعامل والمقاومة. توظيف هذا الإطار كعدسة تحليلية بدلًا من التعامل معه كنموذج معياري، يُتيح للورقة البحثية دراسة كيف تقوم هذه الأنظمة بإعادة توزيع الوضوح والقابلية، التشغيل، السلطة والمسؤولية في قطاع الإغاثة والعمل الإنساني في غزة.

المنهجية

تتبنى هذه الدراسة تصميمًا نوعيًا تفسيريًا لدراسة حالة، يُركز على كيفية تعامل العاملين في قطاع الإغاثة والعمل الإنساني في غزة مع الأنظمة ذات العلاقة بالذكاء الاصطناعي والأنظمة الرقمية، كيف يفهمونها وكيف يتنقلون بينها بالممارسة الفعلية. بدلًا من مسح كافة الأدوات أو إعادة بناء تصميمها الداخلي، تعاين الدراسة الحوكمة التكنولوجية من خلال الروتين الإداري، تبعيات المنصة، إجراءات التحقق، الحذر المؤسساتي، والفهم غير المتكافئ.

بيانات، أخذ عيّنات، ووصول ميداني

تتكون البيانات الأولية من عشر مقابلات شبه منظمة أجريت بين كانون الأول/ ديسمبر 2025 وكانون الثاني/ يناير 2026 مع الموظفين الفلسطينيين داخل غزة، والموظفين الفلسطينيين النازحين إلى مصر أو العاملين منها، والموظفين غير الفلسطينيين من الوكالات الأممية، الجمعيات غير الحكومية الدولية، العاملين في مناصب عملياتية وإدارية. تم إرسال أكثر من خمسين طلب مقابلة إلى وكالات أممية، جمعيات غير حكومية دولية، وجمعيات فلسطينية محلية؛ إلا أن العديد منها لم يحظَ بأي رد، أو تمت إحالتها للمكتب الرئيسي، أو رفض الطلب لأسباب متعلقة بالحساسية المؤسساتية. سبق أن تم اختيار المشاركين بشكل هادف لتغطية التباين في الوظائف، المؤسسات، المواقع، ومدى قربهم من استخدام الممارسات الرقمية والممارسات ذات العلاقة بالذكاء الاصطناعي. على الصعيد الإحصائي، لا تُعتبر العيّنة تمثيلية، لكنها تستخدم لاستبيان سجّل قائم على التحليل إزاء كيف يعيش أصحاب المناصب المؤسساتية ويتعاملون مع هذه الأنظمة. نظرًا لحساسية الإغاثة والعمل الإنساني في غزة، تم إجراء جميع المقابلات دون الكشف عن الهوية، بموافقة شفوية، وسط تعميم للمناصب والانتماءات، وبموجب حدود وضعها المشاركون للحد من المخاطر. كما تم التستر على بعض أسماء الأنظمة، وسيرورات العمل، والإجراءات المؤسساتية من منطلقات أخلاقية. بما أن الحرب والنزوح وانهيار البنية التحتية والقيود الأمنية تحد من الوصول إلى تصميم النظام، قرارات المانحين، والبنى التحتية للبيانات الواقعة تحت سيطرة الجيش، تعتمد الدراسة بشكل انتقائي على وثائق سياسة الإغاثة والعمل الإنساني، الإرشادات الفنية، أوصاف البرامج العامة، والتقارير كدعم سياقي وتفسيري وليس كمنهجية متكافئة.

الإجراء التحليلي

يسترشد التحليل بالإطار المتكامل للورقة البحثية المعنيّ بحوكمة الإغاثة والعمل الإنساني، البيانات ودراسات الذكاء الاصطناعي الحيويّة للدراسة، كما في إطار الحكم الاستعماري الاستيطاني، والاقتصاد السياسي النسوي. ساهمت جهات النظر هذه بتوجيه دليل المقابلة والتحليل، لإجراء المقابلات بحسب الموضوعات المتكررة مثل التصنيف، إتاحة الوصول، التحفّظ الإداري، التحقق، الضبابية والتعتيم، إعادة توزيع العمل، والمخاطر المؤسساتية. جرى تحليل مواد المقابلات بموضوعية، مسترشدين ببراون وكلارك، من خلال الترميز التكراري والقراءة المُقارِنة لكافة مقابلات المشاركين بهدف تحديد الآليات النمطية والتباين المُعتبر في كيفيّة مواجهة الأنظمة الرقمية والأظمة ذات العلاقة بالذكاء الاصطناعي في الممارسة العملية. كما أولينا الاهتمام بالفجوات بين الإدعاءات المؤسساتية الرسمية والتجربة العملياتية اليومية. تم استخدام مواد إضافية فرعية فقط لأغراض وضع السياق وتحليل المقابلات في مواضع اقتضت الحاجة لذلك، وليس كدليل مستقل للادعاءات المُعممة عن تصميم الأنظمة الداخلية أو نشرها واستخدامها على مستوى القطاع.

المقامية والإنعكاسية الذاتية

أجرت الدراسة باحثة فلسطينية تعمل بمقربة من سياق الإغاثة والعمل الإنساني قيد الدراسة، كما أنها تشغل وظيفة جزئية داخلية مما يمنحها قربًا حيويًا. ساهمت اللغة المشتركة، والتجربة المُعاشة تحت وطأة الاحتلال، ومعرفة مؤسسات الإغاثة والمساعدات الإنسانية، في تسهيل الوصول والتفسير. في الآن ذاته تمت مراجعة الإنعكاسية الذاتية طوال الوقت لتجنب التعاطف المُفرط والبقاء متيّقذين لتباين

الأدوار، حدّة الانكشاف، وحدود التمثيل في ظل الحرب والقيود السياسية.

القيود والمصداقية

تستند الدراسة إلى عدد محدود من المقابلات ولا تدعي تمثيل قطاع الإغاثة والعمل الإنساني بشكل قاطع. ومن القيود المفروضة على إتاحة الوصول نذكر مراقبي المعلومات الأمنيين، المخاوف الأمنية، وإعادة التوجيه إلى المقر التنظيمي، حيث لم تنجح الدراسة بمعاينة تصميم المنظومة مُباشرة، ولا عمليات الشبكة الخلفية (Backened) ولا عمليات صنع القرار من قبل المانحين، ولا البنى التحتية للبيانات الخاضعة لسيطرة الجيش. وبالتالي، فإن الدراسة تدرس كيف يواجه طاقم الإغاثة والأعمال الانسانية، الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي في الممارسة الفعلية، وكيف يقومون بتفسيرها والتنقل فيما بينها، بدلًا من البنية المؤسساتية الكاملة التي تدعمها. تعتمد المصداقية على تماسك الأنماط عبر المشاركين في الأدوار والمواقع والمناصب التنظيمية المختلفة، مع اقتصار الادعاءات الأوسع على ما يمكن دعمه ببيانات المقابلة والمواد السياقية المتاحة للجمهور.

النتائج: الذكاء الاصطناعي والحوكمة الرقمية وممارسات الإغاثة والمساعدات الإنسانية اليومية في غزة

عبر المقابلات، يظهر «الذكاء الاصطناعي» في شكلين متشابكين: استخدام الموظفين غير الرسميين للأدوات التوليدية لإدارة عبء العمل، والأنظمة الرقمية العامة القائمة على حوكمة التسجيل والتحقق والاستحقاق والإبلاغ وتداول البيانات (المقابلات 2 و 4 و 5 و 8 و 10). تركز النتائج على أربع ديناميكيات مُتكررة: التبني غير الرسمي على وقع الحوكمة الضعيفة، السيطرة الخارجية على الفئات والقوائم، تحويل العمل والمخاطر إلى أسفل السلسلة القيادية، والتعامل اليومي في ظل ظروف الرعاية والتعرض والمسؤولية المُقيّدة.

تُظهر المقابلات أن الأنظمة ذات العلاقة بالذكاء الاصطناعي والأنظمة الرقمية تدخل في قطاع الإغاثة والعمل الإنساني في غزة بشكل غير متكافئ، من خلال الروتين الإداري، تبعيات المنصة، إجراءات التحقق، والتعامل على المستوى الإداريّ. ليس الإبتكار ولا النجاعة من آثارها الأكثر تماسكًا، بل تكثيف أعمال التصنيف والفرز، الشفافية الجزئية، بيانات مكشوفة على نطاق واسع، وأعباء غير متكافئة للتحقق، التبليغ والامتثال.

1. إستخدام الذكاء الاصطناعي والحوكمة بشكل غير رسمي بموافقة ضمنية صامتة

يدخل الذكاء الاصطناعي العمل اليوم للإغاثة والعمل الإنساني بداية كأداة للتعامل والتكيّف وليس كمشروع ابتكار وتحديث رسمي. وصف المُحاوَرون في المقابلات بشتى منصابهم، كيف يستخدمون أدوات توليدية لإدارة والتعامل مع ضغط العمل، والعمل التنظيمي الإداري، والحفاظ على مستوى الأداء في ظروف متأزمة. وأوضح أحد الأشخاص المُحاوَرين: «أستخدم كل ما يفيدني... بلاكبوكس، جيميني، أي برمجيات مساعِدة... أريد أن أسهّل الأمور على نفسي» (المقابلة 2). كما ربط المُحاوَر ذاته هذا الأمر مُباشرة بالأداء والتوقعّات من قبل الإدارة: «منذ أن بدأت بتوظيف الذكاء الاصطناعي في عملي، صار مديري أسعد مني... تحسن عملي... أستخدمه كمساعد شخصي لي» (المقابلة 2). في الشؤون المالية، تم تأطير الذكاء

الاصطناعي بالمثل على أنه يخفف من الجهد المعرفي على مستوى الميكرو: «بدًلا من التفكير في وظيفة ما ببرنامج الإكسيل [excel]... أطلب من الذكاء الاصطناعي القيام بالعمل» (المقابلة 3). في جميع هذه المُقابلات، يظهر الذكاء الاصطناعي كأداة صمود وبقاء غير رسمية في إطار أنظمة الإغاثة والعمل الإنساني المثقلة أكثر منه تحوّل مؤسساتي استراتيجي (المقابلات 2، 3، 8، 10).

إلا أنه في الآن ذاته، فإن استخدام الذكاء الاصطناعي لم يكن متكافئًا على الصعيد الماديّ. وصفت إحدى المُديرات المُقيمة في غزة الذكاء الاصطناعي بأنه متاح فقط عندما تسمح البنية التحتية بذلك، وحتى عندما تسمح لا يمكن الاعتماد عليه: «لا أملك ارتباطًا قويًا ومستقرًا بالانترنت سوى في المكتب، أستخدم ChatGPT، لكنني أواجه صعوبات جمّة. يحذف ChatGPT نقاطي الأصلية أو يقوم ببساطة بتغيير معلومات مهمة» (المقابلة 10). وقد ربطت هذه القيود بالعمل الميداني مُباشرة، وبأعمال الرعاية وانهيار البُنى التحتية والمنشآت: «عملي ذي طابع ميداني بالغالب، لا أستطيع التركيز، عليّ أن أهتم بالوجبات والطعام، بأطفالي، وبالواجبات المنزلية مع شحّ الكهرباء أو من دون شيء تقريبًا، لا أملك الوقت للذكاء الاصطناعي» (المقابلة 10). وأعرب آخرون عن شكوكهم وتخوّفاتهم الصريحة، لا سيما في أوساط الجمعيات الخيرية المحلية والجمعيات غير الحكومية المحلية، حيث كان يُقرأ الذكاء الاصطناعي على أنه فرصة أقل من كونه نقطة ضعف. قال أحد الأطباء ببساطة: «نتخوّف منه. يجب حظره. كُليًا» (المقابلة 4). في حين أكد آخر أن استخدام الذكاء الاصطناعي في غزة «ليس ناضجًا كفاية» في ظل الظروف الراهنة ويتطلب مراقبة دقيقة للعواقب والتأثير (المقابلة 1). لذلك يبدو أن فهم والتقاط الذكاء الاصطناعي منوط بالمنصب، السياسة التنظيمية، الاتصالية (بشبكة الانترنت) والظروف المعيشية تحت الحصار، ولا ينتشر بشكل متكافئ في رحاب منظومة الإغاثة والعمل الإنساني.

نمط ثانٍ هو عدم التطابق بين التفويض الرسمي والممارسة الفعلية. وصف الموظفون مرارًا وتكرارًا استخدام الذكاء الاصطناعي بأنه غير رسمي، أو يتم تقبله بشكل ضمني أو بصمت، أو يُحظر بشكل انتقائي، أو ببساطة يُترك دون تعريف. وقد عبّر أحد الموظفين المقيمين في غزة عن ذلك صراحة: «نحن نستخدم أدوات أخرى لجزئية التفكير ولعمليات صنع القرار، رسميًا، غير مسموح لنا؛ ولكن بشكل غير رسمي، نستخدم بعض هذه الأدوات للمساعدة في استخراج الأنماط من البيانات، ولاتخاذ القرارات وإصدار توصيات» (المقابلة 5). ووصف آخر الاستخدام واسع النطاق للأدوات غير المُصرّح استخدامها في عمل محاذٍ لاتخاذ القرارات: «يستخدم العديد من الموظفين أدوات الذكاء الاصطناعي خارج القنوات الرسمية أو المُصرّح بها... غالبًا ما يقوم الزملاء بتحميل ملفات إكسيل [Excel] أو قواعد بيانات تحتوي على بيانات شخصية إلى أدوات مثل ChatGPT ويطلبون منهم إجراء التقييم أو تحديد معايير الاستحقاق أو توليد توصيات» (المقابلة 5). على مستوى الجمعيات الخيرية والمؤسسات غير الحكومية المحلية، غالبًا ما برز ذلك على أنه حوكمة غيبية. كما أوضحت مُديرة بقولها «لم يخبرني أحد في مؤسستي بما يتوجب عليّ أن أفعله أو لا أفعله، أستخدمه عندما يكون ذلك مناسبًا» (المقابلة 10).

باختلاف المقابل، أنتج عدم التطابق بين التفويض الرسمي والممارسة الفعلية، نمطًا من الصمت التنظيمي والقواعد الجزئية والإنفاذ غير المتكافئ، وعلى وقعه توّسع توظيف الذكاء الاصطناعي بصيغة غير رسمية في حين ظلت المسؤولية

فردية. التناقض مع هياكل حوكمة تكنولوجيا المعلومات والاتصالات الأكثر رسمية مفيد في هذه الحالة. أكد أحد المُحاوَرين والذي يعمل على الحوكمة والتصاريح أن بعض أدوات الذكاء الاصطناعي كانت غير مُصرّح بها صراحةً لأن التصاريح الضعيفة قد تعرّض معلومات حساسة للكشف أمام «مستخدمين غير المتوقعين وغير مُصرّح» (المقابلة 6). ومع ذلك، حتى هناك، بدت الحوكمة هشة لأنها اعتمدت على النضج التقني، ووعي الموظفين، والحدود القابلة للإنفاذ، مع تفاوت فيما بينها بالمُمارسة الفعلية.

2. التصنيف والتحقق ومقام «المستخدم»

النتيجة الثانية التي خلصت إليها الدراسة، هي أن الموقع الأكثر أهمية للحوكمة القريبة من الذكاء الاصطناعي ليس الابتكار، بل هيكلية التصنيف والتحقق، والتي تساهم في تنظيم الوصول إلى المساعدات. وقد وصف أحد المُحاوَرين الإغاثة والعمل الإنساني مرارًا كقطاع تُنظمه القوائم، الاستمارات، التسجيل القائم على المنصة، عمليات التقييم، وسلاسل التحقق. وفي هذه الهيكلية، غالبًا ما تُمنح الجهات الفاعلة المحلية الفلسطينية مقام «المُستخدمين» العملياتيين لأنظمة ليست هي من قام بتصميمها، ولا تتحكم بها، أو تفهمها بالكامل.

وصف أحد موظفي الجمعيات والمنظمات غير الحكومية المحلية التي تعمل مع وكالة تابعة للأمم المتحدة هذا بوضوح: «إن الإنترنت والمنصة بالكامل ملكهم، ونحن هناك كمستخدمين» (المقابلة 4). موضحًا أن الجهات الفاعلة المحلية لا تملك صلاحية تعديل مبنى البيانات أو أن تقرر أي معلومات تُجمع أم لا: «لا نملك ولوجًا مُحددًا لتعديل أو أن نقرر أي نوع من المعلومات تُجمع... لا نملك إمكانية الولوج أو أي سيطرة» (المقابلة 4). تم توفير التدريب، ولكن لم تتم مشاركة الحوكمة: «ستقوم [وكالة تابعة للأمم المتحدة] بتعريفنا بالنظام، وتقديم التدريبات الفنية [حتى نتمكن] من إدخال البيانات وتحميلها. عدا عن كل ذلك لا نملك أي امكانية للولوج أو السيطرة على المنظومة»(المقابلة 4). ووصفت مُديرة مقيمة في غزة ترتيبًا مشابهًا مع وكالة أخرى تابعة للأمم المتحدة ومنظمة غير حكومية دولية شريكة: «تقدم لنا الأمم المتحدة بالضبط قوائم الأشخاص الذين يجب أن نعمل معهم... نتحقق من القوائم... نسجل جميع المعلومات ونُعيد تقديمها لهم» (المقابلة 10). حددت دورها كموظفة للتحقق من المعلومات ضمن نظام أوسع ذي مُخرجات مرئية جزئية فقط: «استخدمت وكالات الأمم المتحدة هذه المعلومات لإنتاج الخرائط والتقارير... يتم نشر بعض المعلومات والتحفظ على معلومات أخرى، لا نعرف» (المقابلة 10). تُظهر هذه الشهادات مُجتمعة أن العاملين يُمنحون إمكانية الوصول تقنيًا من دون أي سلطة حوكمة مؤثرة.

لا يتعلق موقف «المُستخدم» هذا بالمنصات فحسب، بل يتعلق بكيفية التحكم في استحقاق وإمكانية الوصول من خلال التصنيف. إعتبر العديد من المقابلات أن المساعدات تعمل بموجب قوائم خارجية المنشأ، استمارات التسجيل الذاتي، والتحقق المتقاطع، إلى جانب التحقق من الهُويّة، واستمارات التقييم أو التوصية. في إحدى واجهات المنظمات غير الحكومية المحلية مع [وكالة تابعة للأمم المتحدة]، تم تأطير الرقمنة من خلال التسجيل الذاتي والتدقيق: «هناك استمارة للتسجيل الذاتي، حيث يتسجل المُنتفعون... [نحن] عبارة عن جسر بيننا كمنظمة غير حكومية محلية والمنتفعين» (المقابلة 4). أكد المشارك ذاته على الضغط الذي يحمله هذا التحقق في ظل الشحّ: «مشكلتنا هي أن بعض الأشخاص كانوا

يخدعوننا من خلال التسجيل، وبالتالي علينا التحقق من الهُويّة، كما نستخدم بيانات مجموعات ولكن قدرتنا على القيام بالتدقيق بالهُويّات والتحقق منها محدودة للغاية». وبالتالي يصبح البقاء على قيد الحياة متشابكًا مع التنقل في الفئات بينما تظل الجهات الفاعلة المحلية مسؤولة عن التحقق من الحاجة من خلال قوالب إدارية لم يكن لها دور في تصميمها.

كما تشير المقابلات إلى إحتمال إدراج الذكاء الاصطناعي بشكل غير رسمي في هيكلية التصنيف مما يستدعي التداعيات. وقد وصف أحد المشاركين كيف يقوم زملاء بتحميل ملفات إكسيل (Excel) أو قواعد بيانات في أدوات الذكاء الاصطناعي من أجل «إجراء التقييم أو تحديد معايير الاستحقاق أو إصدار توصيات» (المقابلة 5). وحذر آخر من أن التوصيات التي يولدها الذكاء الاصطناعي قادرة على تشويه تقييم الاحتياجات من خلال اختراع فئات أو الخلط بين فئات رئيسية: «هناك مشاكل كبيرة تُعنى بكيف يقوم الذكاء الاصطناعي بتفسير البيانات... فهو يمزج دائمًا بين الكميات والقياسات كما يخلط بين الأرقام والمسافات وأفراد الأسرة والجنس وما شابه. ويمكنه إنشاء أو توليد بيانات لم تكن موجودة لسد الثغرات» (المقابلة 2). وقد وصفت إحدى المُديرات التسلسل الروتيني لقوائم الإنتاج خارجية المنشأ والتحقق المحليّ: «أتلقى قوائم من [وكالة تابعة للأمم المتحدة] نتحقق من قوائم المُنتفعين، ونزور الأطفال والعائلة، ونتحقق من أنهم الأشخاص الفعليون المستحقين للمساعدات وفقًا للقوائم المُدقق فيها وبموجب أرقام الهوية» (المقابلة 10). تُشير هذه الشهادات إلى صياغة إتاحة الوصول للمساعدات من خلال سلاسل مُبهمة قائمة على التصنيف والتدقيق والتحقق، والتي قد تكون مشوبة بمنطقة وتفكير بمساعدة الآلة بسبب ممارسات الموظفين العادية، وليس من خلال منظومة مكشوفة وقابلة للفحص.

خلال هذه المقابلات، تتحمل الجهات الفاعلة المحلية عبء إنتاج البيانات والتحقق منها بينما تبقى صلاحية التصنيف والتفسير والشفافية في أسفل سلسلة القيادة خاضعة لعوامل خارجية.

3. كشف البيانات، ونقل العمل، والقيود المفروضة على البنية التحتية

النتيجة الثالثة هي أن الحوكمة الرقمية وذات العلاقة بالذكاء الاصطناعي في غزة تنقل العمل والتشغيل والمخاطر أسفل السلسلة القيادية العملية رهن ظروف خطيرة من هشاشة البنية التحتية. وصف المشاركون البيانات بأنها ليست مواد إدارية محايدة، بل كمواد خطرة على الصعيد السياسي. لا تُعنى القضية بالخصوصية نظريًا فقط، بل بكشف البيانات الفلسطينية في بيئة خاضعة للشروط الأمنية، وعدم قدرة الجهات الفاعلة المحلية على معرفة أين تنتقل البيانات بعد جمعها أو التحكم فيها أو الطعن في هذه الممارسات.

وقد أوضح أحد العاملين في الجمعيات الخيرية والمُنظمات غير الحكومية المحلية ذلك بقوله: «أولاً وقبل كل شيء أمن البيانات» (المقابلة 4). كما ربط الأمر بالتدقيق والاستبعاد، مُعربًا عن تخوّفه من «صنع القرار أو التدقيق القائم على تعلم الآلة» وأشار إلى أنه «ليس لدينا مساءلة أسفل السلسلة القيادية» (المقابلة 4). أثار المُحاوَر في المقابلة نفسها مخاوف من الشركات الخارجية (طرف ثالث) المرتبطة بالحكومات الأجنبية وجمع المعلومات الاستخبارية: «أطلعت [وكالة تابعة للأمم المتحدة] مُنظمات فلسطينية غير حكومية أن شركة أمريكية للذكاء

الاصطناعي، معروفة بالعمل مع الجيش الإسرائيلي تحاول تزويدها بالخدمات... رفضنا... لا نملك أية خوادم محلية، وملكيتنا لبياناتنا ضعيفة بأحسن الأحوال، لا نعرف... على أية سحابات»(المقابلة 4). وبالتالي، لا يُفهم موقع السحابة، مُلكية الخادم، ومشاركة المّورد، على أنه اختيار مُحايد للبنية التحتية، بل كمسائل تُعنى بالسيادة وكشف البيانات.

كما ظهرت مخاوف شبيهة في العمل الموجه نحو الحماية. أوضح أحد المشاركين أن المنظمات قد ترغب في حظر استخدام الذكاء الاصطناعي عند التعامل مع مواد ذات حساسية، لكنها لا تملك أي سيطرة على ما يقوم الموظفون بتحميله: «في كثير من الأحيان هناك مواد ذات حساسية... نريد حظر استخدام الذكاء الاصطناعي... ولكن لا يمكنك ضمان عدم قيام الموظفين بتحميل هذه المعلومات» (المقابلة 7). في حين حذّر آخر من أن الاستخدام غير الرسمي للذكاء الاصطناعي ينطوي على «مخاطر جسيمة، إذ يتم تحميل بيانات شخصية حساسة إلى أنظمة قد تعيد استخدام البيانات أو إعادة تدويرها لأغراض التدريب والتعلم» (المقابلة 5). في المقابل، عبّرت إحدى المُحاوَرات عن التطبيع الصارخ مع التجسس تحت الحصار: «الإسرائيليون يراقبوننا ويتتبعوننا طول الوقت، كيف عسى أن يكون ChatGPT أسوأ من ذلك؟» (المقابلة 10). وعليه، يصحّ القول أن المخاطر لا تنبع من سوء الاستخدام فحسب، بل من الافتقار البُنيويّ للسيادة على تدفقات البيانات في بيئة خاضعة لشروط أمنية مُشددة (المقابلات 4 و 5 و 7 و 10).

لا يمكن فصل هذه المخاطر عن نقل العمل. تصف جميع المقابلات الذكاء الاصطناعي والأنظمة الرقمية بأنه ينقل العمل أو يغيّر طابعه بدلاً من تقليله. أشار أحد العاملين في الرصد والتقييم والمساءلة والتعلم (MEAL) إلى أن الشركاء المحليين يجمعون البيانات الميدانية بينما تبقى أعمال مراجعة البيانات في أيدي المقر المركزي: «أعمل مع شركاء محليين يجمعون البيانات في الميدان... وعادة ما أقوم بمراجعة البيانات وتنظيفها بعد شركائي» (المقابلة 3). ولاحظ المُشارك ذاته أن الذكاء الاصطناعي قد يستغرق «وقتًا أطول... أكثر من الطرق التقليدية لجمع البيانات» (المقابلة 3). وصف أحد الموظفين المُقيمين في غزة قيام المانحين بإجبار الفريق على استخدام كوبو (KoBo) كعبء يومي على وقع ضعف الإتصال بالانترنت: «قدم لنا مانحنا هذا البرنامج المتنقل... كوبو (KoBo)... هذا يعني أنني سأضطر إلى استخدامه يوميًا... نحن غير متصلين كثيرًا... اللغة... البرنامج يعلق... يتطلب الاتصال بالانترنت. أقوم بتدوين المعلومات على الأوراق ثم أستخدم كوبو (KoBo) عند الإمكان»(المقابلة 8). في حين وصف مُحاوَر آخر التزامات الإبلاغ المتواصلة طول الوقت: «نحن نقدم... جميع البيانات، على أساس يومي في بعض الأحيان... الأنشطة والمواقع والخدمات الممنوحة» (المقابلة 10). بدلًا من تقليل العمل، في كثير من الأحيان قامت الأنظمة الرقمية بتكرير إدخال المُعطيات، وقدّمت صياغة مُكررة، وإبلاغات متواصلة، وزادت من أعباء التحقق، خاصة في ظل الاتصال غير المستقر.

كان هذا واضحًا بشكل خاص في متطلبات الإبلاغ التي تتطلب أدلة فوتوغرافية في حالات الضائقة. وقد وصف أحد العاملين في غزة ذلك بأنه انتهاك أخلاقي: «يُطلب مني التقاط صور للأنشطة وتحميلها على المنصات... تشعر النساء بالحرج... إذا شعرت بعدم الارتياح حقًا ورفضت شيء ما بشدّة، فلن أفعل ذلك» (المقابلة 8). ما يمكن اعتباره مؤسساتيًا كمحض توثيق، يُعتبر على ارض الواقع كنوع من

الكشف، الإحراج، أو فضيحة أخلاقية.

وزادت هذه الأعباء بسبب الحصار وبنيته التحتية التي يفرضها. لم يكن انقطاع الكهرباء والإنترنت غير المستقر والنزوح وصعوبات الشحن مُجرد ظروف في خلفية العمل، بل هي ظروف دائمة ومستمرة. وقد اعتبر أحد المشاركين «الكهرباء المتقطعة» والتكلفة كعوائق (المقابلة 1). ووصف آخر استحالة الوصول المستقر للانترنت خارج المكتب من أساسه: «بالكاد لدينا إنترنت في غزة... بالكاد أحصل على الإنترنت في خيمتي... من الصعب جدًا بقاء الهواتف الخليوية والحواسيب المحمولة مشحونة» (المقابلة 8). تمكن المُحاوَر ذاته من استخدام ChatGPT «فقط إذا تواجدت بالمكتب، ولكن بضع مرات فقط» (المقابلة 8). في حين ذكر مشارك آخر صراحة أن «جمع البيانات وتقييمها تعطل بشدة بسبب الاتصال غير المستقر بالإنترنت» (المقابلة 5). والنتيجة هي بيئة تكنولوجية طبقية قد يكتسب فيها أولئك الذين لديهم اتصال مستقر بعض مزايا الإنتاجية، في حين أن أولئك الذين هم في حالة نزوح يتحملون تكاليف الامتثال لمتطلبات العمل دون تلقي المعدات والآليات الموعودة.

4. الأعباء الجنسانية، الصوت المحلي، والتعامل اليومي

النتيجة الرابعة هي أن الحوكمة الرقمية وذات العلاقة بالذكاء الاصطناعي يتم التعامل معها وتُعاش عبر العمل القائم على الجندر (النوع الاجتماعي)، وعدم التماثل المعرفي، والتعامل اليومي بدلاً من الامتثال البسيط. وأشارت النساء المُحاوَرات إلى التصادم بين المطالب الرقمية وأعمال الرعاية، حماية الأسرة وبقاءها على قيد الحياة، وعدم الشعور بالراحة على الصعيد الأخلاقي من التوثيق. وقد ربطت إحدى العاملات في الإغاثة والأعمال الإنسانية بين طموحات للتعلّم عن الذكاء الاصطناعي والرغبة بزيادة الدخل، وكيف شطبت هذه الاحتمالات بفعل الحرب وواجب الرعاية: «أتمنى لو كان لدي المزيد من الوقت لتعلم كيفية استخدام الذكاء الاصطناعي لزيادة دخلي، ولكن... عليّ أن أرعى... الواجبات المنزلية... أطفالي دائمًا خائفون ويحتاجون دائمًا إلى الكثير من الرعاية. ليس لدي وقت للذكاء الاصطناعي»(المقابلة 10). وبالتالي، لا يبدو الاقتدار من الذكاء الاصطناعي مجرد مسألة تدريب أو استعداد مؤسساتي على التدريب، بل شحّ الوقت على صعيد جنساني تحت الحصار.

ظهرت نفس الديناميكية في ممارسات التوثيق. وقد وصفت إحدى المُحاوَرات مطالب المانحين بالتوثيق الفوتوغرافي بأنها لا تتوافق والكرامة: «تشعر النساء بالحرج... يجب تصوير الأطفال والنساء بملابس جميلة وعندما يكونون سعداء» (المقابلة 8). ثم صاغت النظام الأوسع على أنه لا علاقة بينه وبين الواقع المُعاش: «يفقد مانحونا وشركاؤنا خارج غزة الاتصال بواقعنا، هل يعرفون أنني أعيش في خيمة؟ هل يعلمون أنه لم يتبقَّ لديّ سوى معطف واحد لأرتديه؟» (المقابلة 8). في العمل الموجه نحو الحماية، ظهرت المخاطر الجنسانية أيضًا فيما يتعلق بالمواد الحساسة واستحالة ضمان عدم الإفصاح: «نحن نعمل على... مواد حساسة... نريد حظر استخدام الذكاء الاصطناعي... ولكن لا يمكنك ضمان ذلك» (المقابلة 7). وبالتالي، فإن الحوكمة الرقمية لا تُعاش فقط كإجراء تقني ولكن كعمل رعاية، وشغل عاطفي، وصراع كرامة في ظل ظروف قائمة على النوع الاجتماعي (الجنسانية) للمسؤولية والكشف (المقابلات 7 و 8 و 10).

نمط مرتبط يُعنى بغياب الصوت المحلي. رأت العديد من المُحاوَرات أن الذكاء الاصطناعي يهدد الهُويّة المؤسساتية والخصوصية المحلية عندما تصبح المخرجات عامة أو شبيهة بالجهات المانحة. وأشارت إحدى المديرات الماليات إلى عواقب ملموسة: «لقد فقدت منحة... بسبب الاستخدام المُفرط للذكاء الاصطناعي في كتابة المُقترحات... لم يعد المُقترح يمثّل هويّتنا وعملنا الجماعي... الجانب المحلي... اختفى... لكنه ليس شيئًا يمكنك إثباته» (المقابلة 7). أما مُحاوَر آخر فقد اعتبر المسألة كقضية سيادة معرفية: «ملكية الفلسطينيين لبياناتهم وحمايتها... نحن بحاجة... [لحماية] المعرفة الحقيقية التي استثمرنا سنوات عديدة في بنائها» (المقابلة 4). ودافع مشارك آخر عن «البنية التحتية الرقمية المملوكة محليًا» كشرط «للاستقلال الرقمي الهادف» (المقابلة 5). تشير هذه التصريحات مُجتمعة إلى احتمال أن تعمل المخرجات المُوّلدة بالذكاء الاصطناعي بشطب الخصوصية المحلية، الصوت المؤسساتي، والمعرفة ذات الخاصية السياقية (المقابلات 4 و 5 و 7).

في الآن ذاته، لا تعرض المُقابلات الموّظفين كمتلقين سلبيين للحوكمة التكنولوجية. وصف المشاركون أشكالًا من العمل الحدوديّ، الرفض، وعدم الامتثال الانتقائي. دعا أحد الموظفين في منظمة محلية غير حكومية إلى الحظر عوضًا عن التبني المنظم: «يجب حظر ذلك. كُليًا» (المقابلة 4). ووصف بالمقابلة ذاتها رفض عرض لتقديم خدمة مرتبطة بالذكاء الاصطناعي من جهة خارجية لأسباب سياسية وأمنية: «تم رفض... بالانتير أيه أي (Palantir AI)» (المقابلة 4). في حين رأت مُشاركة أخرى أن الرفض عمليّ مُتضمن وليس أيديولوجيًا: «إذا شعرت بعدم الارتياح حقًا وأعارض شيئًا ما بشدة، فلن أفعل ذلك» (المقابلة 8). على مستوى المُنظمات الدولية غير الحكومية، قد يظهر العمل الحدودي أيضًا من خلال اللغة الإجرائية حول الحقوق الرقمية وحماية البيانات، حتى عندما يستمر الاستخدام غير الرسمي بالتوازي (المقابلة 3). لا ترقى هذه الإجراءات إلى مستوى السيطرة المؤسساتية التامّة، ولكنها تُظهر أن الذكاء الاصطناعي بالعمل الانساني يُصاغ من خلال الأحكام الأخلاقية المُشتتة تحت ظروف غير متكافئة.

مُباحثة: الذكاء الاصطناعي والحوكمة والسلطة في نظام العمل الإنساني بغزة

في العمليات الإنسانية ذات العلاقة بغزة، لا يعمل الذكاء الاصطناعي كابتكار تكنولوجي بقدر ما يُوظّف كآلية حوكمة تعيد تنظيم الوضوح والقابلية، التشغيل، والسلطة في ظل القيود الاستعمارية. تجيب النتائج على أسئلة الورقة الثلاثة بطرق مترابطة. أولًا، يواجه الموظفون الأنظمة ذات العلاقة بالذكاء الاصطناعي والأنظمة الرقمية بشكل أساسي كبنى تحتية للحوكمة اليومية مدمجة في الروتين الإداري، وتبعيات المنصة، والتعامل مع الأزمات. ثانيًا، تصوغ هذه الأنظمة شكل التنسيق، اتخاذ القرارات، وتوزيع المساعدات من خلال هياكل التصنيف، سلاسل التحقق، أنظمة الإبلاغ، وسيل العمل المُعتمد على المنصة، والتي تركز السُلطة أعلى السلسلة القيادية مع نقل التشغيل والعمل والمخاطر إلى أسفل السلسلة. ثالثًا،

تفسر الجهات الفاعلة في الخطوط الأمامية هذه الأنظمة وتتعامل معها وأحيانًا تعترض عليها من خلال الاستخدام الانتقائي، فرض حدود أخلاقية، رفض الاستخدام، والتأقلم القائم على البقاء والصمود تحت الحصار وعدم التماثل المؤسساتي. ينتج عن كل ذلك، تجمّع مُجزّأ تُمارس من خلاله السلطة الإنسانية ويُعاد توزيع الأعباء الإدارية.

مما يؤول بالتحليل بعيدًا عن روايات الابتكار، وباتجاه الحوكمة. القضية الرئيسية ليست ما إذا كانت المُنظمات «تستخدم الذكاء الاصطناعي» بشكل رسمي، بل كيف تصوغ هذه الأنظمة التكنولوجية القابلية والوضوح، التصنيف، إمكانية الطعن، والتحقق. إضفاء صفة رسمية على الحوكمة ليس إلا جزئيًا في جميع النتائج والمُخرجات. قد تكون هناك سياسات حول الأدوات المُصرّح بها، وحماية البيانات، والاستخدام المسؤول، ألا أنه في الممارسة العملية غالبًا ما تتم حوكمة الأنظمة ذات العلاقة بالذكاء الاصطناعي بواسطة قواعد جزئية، صمت تنظيمي، وإنفاذ غير متكافئ. هذا ما تعتبره النتائج موافقة ضمنية صامتة: تتوّسع الأساليب الالتفافية غير الرسمية إلى مهام تترتب عليها عواقب، في حين تُدفع المسؤولية أسفل السلسلة القيادية. لا تعمل الحوكمة بواسطات مداولات شفافة وواضحة، بل تميل للعمل بموجب إمتثال مُشتت، وسلطة أعلى سلسلة القيادة، وسلاسل قرار مُبهمة.

تُظهر القراءة النازعة للاستعمار أن هذه الديناميكيات تتكشف داخل مجال مُنظم بواسطة سيطرة خارجية مفروضة على الحركة والتنقل، البنية التحتية، إتاحة الوصول ومدى الرؤية. يُعتبر الذكاء الاصطناعي في غزة مهمًا كونه يعزز ويشحن العلاقات القائمة بين الحكم البيروقراطي والاستعماري. تلعب الجهات الفاعلة المحلية دور مزوّدي بيانات، مدققين، مستخدمين عملياتيين، وليس كأصحاب سلطة على الفئات التي تُحدد الحاجة بوضوح. فهم يُدخلون المعلومات، يراجعون القوائم، ويحافظون على سيل العمل، بينما تظل معايير اتخاذ القرار، التفسير أسفل السلسلة القيادية والتحكم بالبنية التحتية بأيادٍ خارجية. وهذا ينتج اعتمادًا معرفيًا وبنيويًا: يتحمل أولئك الأقرب إلى الواقع المُعاش عبء جعله مقروءًا دون أن يملكوا أي سلطة إزاء كيفية تصنيفه أو تفسيره أو التصرف بموجبه. مما يُفسر لماذا الطعن المُقيّد والمحدود مركزيّ للنتائج. غالبًا ما تُترجم المُساءلة والمُحاسبة إلى الامتثال بدلًا من المُشاركة المؤثرة في صنع القرار. الموظفون مسؤولون عن إدخال البيانات، مراجعتها وتنظيفها، والتحقق منها؛ إلا أنه غالبًا ما لا يكون واضحًا لهم كيف تُنتج هذه القوائم، أو كيف تُحدد المعايير، أو كيف تصوغ الفئات وتؤثر على شكل النتائج النهائية. وعليه، ما يبدو كمُجرد إجراء تقني هو أيضًا توزيع للسُلطة.

تُظهر قراءة اقتصادية سياسية نسوية أن هذه الأنظمة تعيد تنظيم العمل بطرق مشوبة بلغة الكفاءة. العمل المكثف في مجال البيانات ليس تقنيًا فحسب، بل هو أيضًا عمل رعاية، عمل عاطفي، وتحمل مسؤولية تتم تحت ظروف مؤسساتية غير متماثلة. غالبًا، وبشكل غير متكافئ، ما تكون النساء، لكونهم أقرب للأسر والمجتمعات، هن من يقمن بعمليات التحقق، المتابعة، التوثيق، والمحاولات المتكررة للحفاظ على الوضوح في ظروف متأزمة. يُظهر تباين وشحّ الوقت القائم على الجنس، الصراعات حول التوثيق المعنية بمسألة الكرامة والحشمة، والضغط لإدارة بقاء وسلامة الأسرة جنبًا إلى جنب مع التقارير المؤسساتية أن الامتثال

الرقمي يُختبر ويُعاش من خلال التكاثر الاجتماعي بقدر ما يُعاش من خلال العمل الرسميّ. بكل بساطة، الذكاء الاصطناعي والأنظمة الرقمية لا يوّفران الوقت. بل إنها تنقل العمل أسفل السلسلة القيادية داخل المؤسسات وتجعل هذا العمل بارزًا وواضحًا بدرجات أقل.

لا يمكن فصل هذه الأعباء عن ظروف البنية التحتية والظروف السياسية. إذ يُشكل الحصار، النزوح، والاتصال غير المستقر بالانترنت، إضافة إلى الاعتماد على المنصات الخاضعة للسيطرة الخارجية، ما تستطيع الأنظمة التكنولوجية فعله، ولمصلحة من، وبأي ثمن. تعد الحوكمة الرقمية بالسرعة والاتساق والوضوح والقابلية، ولكنها غالبًا ما تنتج ازدواجية، تأخيرات، وتزيد من أعباء التنسيق، علاوة على التنازلات الأخلاقية في ظل ظروف يصعب فيها الحفاظ على الوضوح ذاته. مما يُنتج نظامًا تكنولوجيًا يعتمد على مُخرجات (نتائج) معيارية في حين يتم العمل وسط ظروف تقوّض باستمرار إمكانية إنتاجها بأمان أو بدقة.

أخيرًا، تُعقّد النتائج أي قراءة للفاعلين في الخطوط الأمامية كمتلقين سلبيين أو كمُستخدمين مُتمكنين من التكنولوجيا. يفسر العاملون في المجال الإنساني هذه الأنظمة ويتعاملون معها ويتنقلون بينها وأحيانًا يرفضونها في الممارسة العملية. هم يضعون الحدود، ويرفضون أدوات مُعيّنة، يتعاملون ويلتفون على المطالب المُسيئة، ويصدرون أحكامًا أخلاقية تحت الضغط. لكن هذه المسؤولية تبقى مُجزأة وتحت قيود. فهذه المسؤولية لا تُلغي التماثل الأوسع نطاقًا والذي يحتفظ من خلاله الفاعلون الخارجيون بسُلطة غير متناسبة على البنى التحتية والفئات ومعايير الأدلة. بل هي تُوضّح أن الذكاء الاصطناعي في العمل الإنساني لا يخضع عمليًا لسلطة السياسة الرسمية فحسب، بل أيضًا يخضع للأحكام المتباينة، ويُرفض، ويتم التأقلم والتكيّف معه على أساس البقاء على قيد الحياة.

تدعم النتائج مُجتمعة الإدعاء الأوسع نطاقًا: في العمليات الإنسانية ذات العلاقة بغزة، يعمل الذكاء الاصطناعي كآلية حوكمة تُعيد تنظيم الوضوح والقابلية، التشغيل، والسلطة في ظل القيود الاستعمارية. يدخل الذكاء الاصطناعي عبر مسارات مُجزأة، ولا يتم تبنيه بشكل متماسك ومكتمل، وتتم حوكمته من خلال المخاطر والامتثال وليس من خلال سلطة تشاركية. كما أنه يُختبر ويُعاش من خلال أعباء التحقق، التبعية المعرفية، هشاشة البنية التحتية، والتعامل غير المتكافئ. هذا يُعيد تأطير الذكاء الاصطناعي في العمل الإنساني بعيدًا عن مخزون الأدوات الصالح وقوائم مراجعة الأخلاقيات، ويؤطره باتجاه سؤال ذي طابع سياسي بدرجة اكبر بكثير: من يحدد الفئات؟ ومن يتحمل عبء جعل الحاجة واضحة وقابلة؟ ومن يمكنه الطعن في التصنيفات المُسيئة؟ وكيف تُثبت السلطة التكنولوجية في حين أكثر الناس تآذيًا منها يبقون الأقل قدرة على صياغة شروطها.

الخاتمة والعواقب المُترتبة على السياسة

تناولت هذه الورقة كيف تدخل الأنظمة الرقمية والأنظمة ذات العلاقة بالذكاء الاصطناعي على قطاع العمل الإنساني في غزة، كيف تتم حوكمتها، وكيف يتم التعامل معها وتُعاش، في ظل ظروف تحت الحصار، التجسس، وكونها خاضعة للسيطرة الخارجية. بموجب الأدلة، يبدو أن الذكاء الاصطناعي ليس عبارة عن أجندة

ابتكار مُوّحدة، بل كنظامين متشابكين: قيام الموظفين باستخدام الأدوات التوليدية بشكل غير رسمي لأجل التعامل مع الضغط الإداري وإدارته؛ والأنظمة الرقمية المؤسساتية المُستخدمة لتنظيم الاستحقاق، التحقق، الإبلاغ، وتداول البيانات الإنسانية. في الاغاثة والعمل الإنساني المعنيّ بغزة، لا يُعدّ الذكاء الاصطناعي في المقام الأول تطورًا تكنولوجيًا، بل إنه آلية حوكمة تُعيد تنظيم الوضوح والقابلية، التشغيل، والسلطة في ظل ظروف القيود الاستعمارية. لا تكمن أهميته في التجديد التقني، بل في دوره المساهم بتكثيف التصنيف، وتوسيع تداول البيانات من دون سلطة عليها أو سيادة؛ وإعادة توزيع العمل والمخاطر والمسؤولية عبر سلسلة تشغيلية غير متكافئة.

تتمثل المساهمة الأساسية للورقة في إعادة صياغة الذكاء الاصطناعي في العمل الإنساني بعيدًا عن قوائم المخزون وقوائم مراجعة الأخلاقيات وباتجاه الحوكمة في حيّز الإغاثة الانسانية القائم تحت الاستعمار. وبالتالي فإن الأسئلة المركزية لا تُعنى بمحض الأدوات الجاري توظيفها واستخدامها، بل تُعنى بمن المسؤول عن تحديد الفئات، ومن يتحكم في القوائم ومنطق التحقق، ومن يمكنه حماية تدفقات البيانات أو الاعتراض عليها، ومن يتحمل العبء عند فشل الأنظمة. تُظهر النتائج أن المساءلة تُترجم في كثير من الأحيان إلى الامتثال بينما تظل القدرة على الاعتراض والطعن مُقيّدة بشكل بُنيويّ، على أن تُوّزع هذه الأعباء بشكل غير متكافئ على المستخدمين كل بحسب الموقع، المنصب، والجنس. على خلفية الظروف المذكورة، يُقابَل ويوازن وعد الذكاء الاصطناعي بالكفاءة مرارًا وتكرارًا بالتحقق المُستخرج، بالتعلّق المعرفيّ، وبتثبيت السلطة الخارجية من خلال إنتاج مخرجات واضحة وقابلة للقراءة.

العواقب المُترتبة على السياسة

بادئ ذي بدء، يجب التعامل مع حوكمة الذكاء الاصطناعي في العمليات ذات العلاقة بغزة على أنها حوكمة التصنيف والوصول، وليس مجرد استخدام آمن للأدوات. عندما تقوم ممارسات الذكاء الاصطناعي أو الممارسات القريبة من الذكاء الاصطناعي بصياغة وتشكيل الاستحقاق، التقييم، وتشكيل القوائم أو التوصيات، يتوجب أن تتم حوكمتها كوظائف توزيعية لاتخاذ القرارات مع معايير مُوّثقة، ذات أصحاب قرار مُحددين، ومسؤولية واضحة عن الآثار المترتبة في مراحل لاحقة. يصبح هذا الأمر مُلّحًا على وجه الخصوص حينما يتوسع الاستخدام غير الرسمي من خلال ما تشخّصه الورقة البحثية الراهنة كموافقة صامتة.

ثانيًا، يجب أن تشمل امكانية الطعن أو الاعتراض العملياتي. تتحمل الجهات الفاعلة المحلية حاليًا مسؤولية إدخال البيانات والتحقق منها وانضباط سير العمل بينما تفتقر إلى الوضوح في كيفية اتخاذ القرارات في المراحل اللاحقة. لذلك يجب أن تتضمن ترتيبات الحوكمة آليات عملية للاستعلام عن التصنيفات، الإبلاغ عن عدم التطابق، تصحيح الأخطاء، والطعن في المعايير المُسيئة من دون أن تترّتب عليه أية عمليات انتقام أو عواقب. يجب أيضًا مطابقة المسؤولية مع السلطة: إذا قامت المنظمات الفلسطينية والموظفون في غزة بإنتاج البيانات والتحقق منها، فيجب أن يكون لديهم تأثير واضح ومُحدد على خانات البيانات، تصميم الفئات، متطلبات الإبلاغ وتفسير المخرجات.

ثالثًا، يجب التعامل مع حماية البيانات على أنها مُشكلة سياسية تتعامل معها

الحوكمة الخاضعة للحصار وليس على أنها امتثال عام. يجب أن يكون تقليل البيانات الحالة المبدئية، وأن يكون الحفاظ على البيانات محدودًا بصرامة، كما يجب على المؤسسات أن تحدد بوضوح موقع تخزين البيانات، ومن يمكنه الوصول إليها وأية موردين أو البنى التحتية السحابية المعنية. حيث يُشترط إجراء فحص بيومتري أو فحص مرتبط بالهُويّة كشرط للوصول إلى المُساعدات، تصبح المشكلة بُنيويّة مُتجذرة وليس محض عملية إجرائية.

رابعًا، يجب أن يعالج التصميم العملياتي مسائل نقل العمل، هشاشة البنية التحتية، والمس بالكرامة كمخاوف تتعلق بالحوكمة وليس كآثار جانبية للتطبيق. تُبيّن النتائج أن الذكاء الاصطناعي والأنظمة الرقمية غالبًا ما تخلق ازدواجية، وإبلاغ متواصل، وتوثيق مشحون بأعباء أخلاقية، في ظل عدم استقرار الاتصال والنزوح المتواصل. وعليه، يتوجب على الأنظمة أن تقلل من متطلبات التحقق والإبلاغ غير الضرورية، وأن تمنح أولية لسيل عمل غير متصل بالانترنت أو ذات النطاق الترددي المُنخفض؛ كما عليها أن تزيل توقعات الدلائل المُهينة والمُسيئة، بشكل خاص ممارسات التوثيق التي تُعرّض النساء أو الأطفال أو الأسر النازحة للإهانة أو الإحراج أو لإساءة أخلاقية.

أخيرًا، يتوجب على مؤسسات ومُنظمات العمل الإنساني التعامل مع التبعية المعرفية وتراجع الصوت المؤسساتي المحلي كمخاطر تتعرض لها الحوكمة. يمكن أن تؤدي المخرجات التي يولدها الذكاء الاصطناعي إلى تبسيط السياق وتجريده، توحيد اللغة، وإضعاف الخصوصية المحلية، بينما تظل البنى التحتية الرقمية خاضعة للتحكم الخارجي. وعليه، يترتب عليها حماية معايير مراجعة المعرفة السياقية والهُويّة المؤسساتية، كما التعامل مع البنية التحتية الرقمية الخاضعة للحكم المحلي ليس على أنها تفضيل تقني بل كشرط للاستقلال الرقمي المُعتبر.

المراجع

- Ananny, Mike, and Kate Crawford. 2018. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." New Media & Society 20 (3): 973–89. https://doi.org/10.1177146144481667664 5/.
- Beduschi, Ana. 2022. "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks." International Review of the Red Cross 104 (919): 1149–69.
- Birhane, Abeba. 2020. "Algorithmic Colonization of Africa." Scripted 17 (2): 389–409.
- Braun, Virginia, and Victoria Clarke. 2006. "Using Thematic Analysis in Psychology." Qualitative Research in Psychology 3 (2): 77–101.
- Burrell, Jenna. 2016. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." Big Data & Society 3 (1): 1–12. https://doi.org/10.1177205395171562251 2/.
- Coppi, Giulio, Rebeca Moreno Jimenez, and Sofia Kyriazi. 2021. "Explicability of Humanitarian AI: A Matter of Principles." Journal of International Humanitarian Action 6 (1): 19. https://doi.org/10.1186/s410186-00096-021-.
- Couldry, Nick, and Ulises A. Mejias. 2019a. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press.
- Couldry, Nick, and Ulises A. Mejias. 2019b. "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?" Internet Policy Review 8 (2): 1–24. https://doi.org/10.147632019.2.1411/.
- Devidal, Pierrick. 2024. "Machine Learning and Humanitarian Forecasting." Humanitarian Data Studies Review 9 (1): 55–78.
- D'Ignazio, Catherine, and Lauren F. Klein. 2020. Data Feminism. Cambridge, MA: MIT Press.
- Donini, Antonio, and Daniel Maxwell. 2013. "From Face-to-Face to Face-to-Screen: Remote Management, Effectiveness and Accountability of Humanitarian Action in Insecure Environments." International Review of the Red Cross 95 (890): 383–413. https://doi.org/10.1017/S1816383114000265.
- Duffield, Mark. 2007. Development, Security and Unending War: Governing the World of Peoples. Cambridge: Polity.
- Eubanks, Virginia. 2018. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press.
- Feldman, Ilana. 2008. Governing Gaza: Bureaucracy, Authority, and the Work of Rule, 1917–1967. Durham, NC: Duke University Press.
- Fraser, Nancy. 2016. "Contradictions of Capital and Care." New Left Review 100 (July–August): 99–117.
- Geiss, Robin. 2021. Protection of Data in Armed Conflict. Geneva: Geneva Academy.
- GPPi. 2021. Research on the Specific Risks or Constraints Associated with Humanitarian Data Sharing with Donors. Berlin: Global Public Policy Institute.
- Grote, Tatjana. 2025. "Data Protection in Humanitarian Action: Military Personal Data Processing." EJIL: Talk!, November 11, 2025.
- Hilhorst, Dorothea. 2010. "Humanitarian Space as Arena: A Perspective on the Everyday Politics of Aid." Development and Change 41 (6): 1117–39. https://doi.org/10.1111/j.14677660.2010.01673-.x.
- ICRC. 2021. "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach." International Review of the Red Cross 102 (913): 463–79. https://doi.org/10.1017/S1816383120000454.
- Jacobsen, Katja Lindskov. 2015. The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity. London: Routledge.
- Latonero, Mark. 2019. "Stop Surveillance Humanitarianism." New York Times, July 11, 2019.
- Madianou, Mirca. 2019. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." Social Media + Society 5 (3): 1–13. https://doi.org/10.11772056305119863146/.
- Said, Edward W. 1978. Orientalism. New York: Pantheon Books.

- Scott, James C. 1985. Weapons of the Weak: Everyday Forms of Peasant Resistance. New Haven, CT: Yale University Press.
- Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. "Between Surveillance and Recognition: Rethinking Digital Identity in Aid." Big Data & Society 8 (1): 1–7. https://doi.org/10.1177205395172110067 44/.
- Wolfe, Patrick. 2006. "Settler Colonialism and the Elimination of the Native." Journal of Genocide Research 8 (4): 387–409. https://doi.org/10.1080146235206010562 40/.
- .org/10.11453593013.3594073/.
- Conley, Julia. 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians'. Truthout, 19 May 2024. https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/.
- Davies, Harry. 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data'. The Guardian, 10 August 2025. https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data.
- Davies, Harry, and Yuval Abraham. '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'. The Guardian, 6 August 2025. https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.
- Davies, Harry, and Yuval Abraham. 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'. The Guardian, 25 September 2025. https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israel Demanded Google and Amazon Use Secret "Wink" to Sidestep Legal Orders'. The Guardian, 29 October 2025. https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'. The Guardian (Jerusalem), 6 March 2025. https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.
- Davies, Harry, and Yuval Abraham. 'Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War'. The Guardian (Jerusalem), 23 January 2025. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.
- Davies, Harry, and Bethan McKernan. 'Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse'. The Guardian, 5 April 2024. https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse.
- De Luce, Dan. 'Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies'. NBC News, 20 September 2024. https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888.
- Decoster, Xavier Stephane, Ilhab Jebari, Anat Lewin, and Carlo Maria Rossotto. The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development. No. 104263. World Bank Group, 2016. http://documents.worldbank.org/curated/en/993031473856114803.
- Demopoulos, Alaina. 'Honk Honk! Can Noise Cameras Reduce "Potentially Fatal" Sound Pollution?' The Guardian (New York), 4 October 2023. https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras.
- Electronic Frontier Foundation. 'Gunshot Detection'. Street Level Surveillance, n.d. https://sls.eff.org/technologies/gunshot-detection.
- Euro-Med Human Rights Monitor. Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies. 13 November 2022. https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles,-stop-fully-cooperating-with-security-agencies.
- Fathallah, Sarah. 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine'. Public Humanities 2 (2026): e7. https://doi.org/10.1017/pub.2025.10113.
- Fathallah, Sarah. 'Artificial Intelligence and the Orchestration of Palestinian Life and Death'. Tech Policy Press, 12 August 2025. https://www.techpolicy.press/artificial-

intelligence-and-the-orchestration-of-palestinian-life-and-death/.

- Fathallah, Sarah, and Nick Mitchell. 'Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life'. Disjunctions Magazine, January 2026. https://disjunctionsmag.com/articles/occupied-assets/.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 'From Data Mining to Knowledge Discovery in Databases'. AI Magazine, 15 March 1996.
- Flensburg, Sofie, and Signe Sophus Lai. 'Follow the Data! A Strategy for Tracing Infrastructural Power'. Media and Communication 11, no. 2 (2023). https://doi.org/10.17645/mac.v11i2.6464.
- Frenkel, Sheera, and Natan Odenheimer. 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns'. The New York Times, 25 April 2025. https://www.nytimes.com/202525/04//technology/israel-gaza-ai.html.
- Front Line Defenders. OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. Front Line Defenders, 2021. https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware.
- Goodfriend, Sophia. The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2021. https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf.
- Goodfriend, Sophia. 'When Palestinian Political Speech Is "Incitement"'. Jewish Currents, 15 September 2021. https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.
- Grim, Ryan, and Waqas Ahmed. 'The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal'. Drop Site, 23 January 2025. https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.
- Halabi, Usama. 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.43249780203845967/.
- Hassan, Zaha, and H. A. Hellyer. Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel. Oneworld Academic, 2024.
- Human Rights Watch. Questions and Answers: Israeli Military's Use of Digital Tools in Gaza. 10 September 2024. https://www.hrw.org/news/202410/09//questions-and-answers-israeli-militarys-use-digital-tools-gaza.
- Human Rights Watch. Spyware Used to Hack Palestinian Rights Defenders. 8 November 2021. https://www.hrw.org/news/202108/11//spyware-used-hack-palestinian-rights-defenders.
- IMEU. Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement. Institute for Middle East Understanding, 2021.
- Investigate. 'Amazon.Com Inc.' The American Friends Service Committee, 7 August 2024. https://investigate.info/company/amazon.
- Investigate. 'Microsoft Corp.' The American Friends Service Committee, 29 January 2025. https://investigate.info/company/microsoft.
- James, Robin. 'Acousmatic Surveillance and Big Data'. Sounding Out!, 20 October 2014. https://soundstudiesblog.com/201420/10//the-acousmatic-era-of-surveillance/.
- Jamil, Yassin. '"Tafāṣīl Muḏhila ʿan Ṭuruq Wa ʾasālīb al-Murāqaba as-Sirrya al-Isrāʾīlya Lil-Hawātif al-Jawwāla Lil-Muqāwama al-Filsṭīnya Wal-Lubnānya" تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel's Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]'. Rai Alyoum, 21 June 2016. https://www.raialyoum.com/تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة-ا/.
- Kelley, Hannah. 'Dual-Use Technology and U.S. Export Controls'. CNAS Technology Policy Lab, 15 June 2023. https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.
- Leix Palumbo, Daniel, and Robert Prey. 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice'. Big Data & Society 11, no. 4 (2024): 20539517241297889. https://doi.org/10.11772053951724129788 9/.
- Leufer, Daniel. 'Sonic Surveillance: Why You Don't Want AI Snooping on You'. Access Now, 23 September 2025. https://www.accessnow.org/ai-snooping/.

- Ludwig, Mike. 'Microsoft Faces Reckoning for Assisting Israel's Genocide in Gaza'. Truthout, 3 December 2025. https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/.
- Mahmoud, Khalid Walid. 'Voiceprint: From a Verification Tool to a Tracking Technology'. The Peninsula, 19 January 2025. https://thepeninsulaqatar.com/opinion/192025/01//voiceprint-from-a-verification-tool-to-a-tracking-technology.
- Mann, Yuval, and Korin Elbaz-Alush. 'Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says'. YNet, 27 June 2023. https://www.ynetnews.com/business/article/hjmohud002.
- Marciano, Avi. 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity'. Surveillance & Society 19, no. 1 (2021): 85–88. https://doi.org/10.24908/ss.v19i1.14543.
- Masarwa, Lubna. 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'. Middle East Eye (Jerusalem), 15 November 2021. https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.
- McClain, Jade. 'Alexa, Am I Happy? How AI Emotion Recognition Falls Short'. New York University, 18 December 2023. https://www.nyu.edu/about/news-publications/news/2023/december/alexa--am-i-happy--how-ai-emotion-recognition-falls-short.html.
- Mhawish, Mohammed R. 'Watched, Tracked, and Targeted'. New York Magazine, 3 December 2025. https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html.
- Microsoft. 'Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza'. Microsoft On the Issues, 15 August 2025. https://blogs.microsoft.com/on-the-issues/202515/05//statement-technology-israel-gaza/.
- Microsoft. Microsoft to Launch New Cloud Data Center Region in Israel. 22 January 2020. https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/.
- Microsoft. What Is the Speech Service? 5 November 2025. https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview.
- Mitnick, Josh. 'Here's How the Israeli Army Is Embracing Digital Transformation'. CIO, 8 February 2020.
- Mossad, Marco. 'Are Global Tech Giants Facilitating Israel's War on Gaza?' Al Majalla, 31 May 2024. https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza.
- Mossad, Marco. 'Voiceprint Technology: A Commercial Hit with Military Utility'. Al Majalla, 7 February 2024. https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility.
- Mullett, Layne. 'Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide'. American Friends Service Committee, 23 July 2025. https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide.
- Niang, Sophie Marie. 'In Defence of What's There: Notes on Scavenging as Methodology'. Feminist Review 136, no. 1 (2024): 52–66. https://doi.org/10.1177/01417789231222606/.
- Nissenbaum, Helen. 'Accountability in a Computerized Society'. Science and Engineering Ethics 2, no. 1 (1996): 25–42. https://doi.org/10.1007/BF02639315.
- No Azure For Apartheid. The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200. 25 September 2025. https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b.
- O'Brien, Danny, and Jillian C. York. 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?' Electronic Frontier Foundation, 11 November 2015. https://www.eff.org/deeplinks/201511//palestine-3g.
- O'Carroll, Lisa. 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'. The Guardian, 4 December 2025. https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf.
- Oslo Accords. Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II). 1995. https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.
- Palestine Today. '"Kayfa tatanaṣṣat ālmuḫābarāt āl'isrāīlya ʿalā jawwālik āšaḫsy!?" كيف تتنصت المخابرات الإسرائيلية على جوالك الشخصي؟! [How does Israeli intelligence eavesdrop on your personal mobile phone?!]'. Palestine Today,

30 December 2013. https://paltodaytv.com/post/466/كيف-تتنصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي.

- Privacy International. The Global Surveillance Industry. 2016. https://privacyinternational.org/sites/default/files/201712-/global_surveillance_0.pdf.
- Reuters. 'Israeli Defense Ministry Launches COVID-19 Voice-Test Study'. Reuters (Jerusalem), 24 March 2020. https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/.
- Reuters. 'Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to $3 Billion, Report Says'. 30 December 2025. https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-202530-12-/.
- Sada Social. Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military. 18 May 2024. https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdmy-oatsab-l-algysh-alsrayly.
- Sa'di, Ahmad H. Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority. Manchester International Relations. Manchester University Press, 2016.
- Salah, Hana. '"Albaṣma as-Ṣaūtya" Adāt Isrā'īl Litanfīḏ Syāsat "Attaṣafya al-Jasadya" "البصمة الصوتية" أداة إسرائيل لتنفيذ سياسة "التصفية الجسدية" ["Voiceprints": Israel's Tool for Implementing "Elimination"]'. Al-Monitor, 4 February 2014. https://www.al-monitor.com/ar/contents/articles/originals/201402//gaza-israel-islamic-jihad-hamas-mobile-war.html.
- Salah, Mohamad Ateyyah, Mohamad Shalodi, and Mahmoud Skafi. 'Voiceprint Authentication System'. Palestine Polytechnic University, 2021. https://scholar.ppu.edu/bitstream/handle/1234567897547//Voiceprint-Authentication-System.pdf.
- Shalhoub-Kevorkian, Nadera. Security Theology, Surveillance and the Politics of Fear. 1st edn. Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781316159927.
- Shalhoub-Kevorkian, Nadera, and Abeer Otman. 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023. Secrecy as Colonial Violence.
- Siddiqui, Usaid. '"Chilling Effect": Israel's Ongoing Surveillance of Palestinians'. Al Jazeera, 8 May 2023. https://www.aljazeera.com/news/20237/5//chilling-effect-israels-ongoing-surveillance-of-palestinians.
- Smalley, Suzanne. 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker'. The Record, 20 November 2025. https://therecord.media/nso-seeks-to-overturn-whatsapp-case.
- Smith, Brad. 'Update on Ongoing Microsoft Review'. Microsoft On the Issues, 25 September 2025. https://blogs.microsoft.com/on-the-issues/202525/09//update-on-ongoing-microsoft-review/.
- Stanley, Jay. 'On the Creation of Giant Voiceprint Databases'. ACLU, 16 October 2014. https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases.
- Swinhoe, Dan. AWS Launches Israeli Cloud Region in Tel Aviv. 2 August 2023.
- Tawil-Souri, Helga. 'Digital Occupation: Gaza's High-Tech Enclosure'. Journal of Palestine Studies 41, no. 2 (2012): 27–43. https://doi.org/10.1525/jps.2012.XLI.2.27.
- Tawil-Souri, Helga. 'Hacking Palestine: A Digital Occupation'. Al Jazeera, 9 November 2011. https://www.aljazeera.com/opinions/20119/11//hacking-palestine-a-digital-occupation.
- Tawil-Souri, Helga. 'Israel's Telecommunications Lines and Digital Surveillance Routes'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023.
- Tawil-Souri, Helga. 'Surveillance Sublime: The Security State in Jerusalem'. Jerusalem Quarterly, no. 68 (December 2016): 56–65. https://doi.org/10.70190/jq.I68.p56.
- The Office of the High Commissioner for Human Rights. 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. A/HRC/592025 .23/. https://www.ohchr.org/en/documents/

country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur.

- The Palestine Chronicle. 'Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media'. 18 February 2026. https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/.
- The Times of Israel. 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'. The Times of Israel, 26 April 2025. https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.
- Zureik, Elia. 'Colonialism, Surveillance, and Population Control'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.43249780203845967/.
- Zureik, Elia, and David Lyon. 'Coronavirus Surveillance and Minority Groups in Israel/Palestine'. The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.
- Zureik, Elia T. Israel's Colonial Project in Palestine: Brutal Pursuit. Routledge Studies on the Arab-Israeli Conflict 20. Routledge, 2016.

ialiis@birzeit.edu
ialiis.birzeit.edu

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