

أصوات أسيرة:

التجسس الصوتي الخوارزمي في فلسطين

ورقة بحثية ضمن كتاب

”
الهيمنة الرقمية: الذكاء الاصطناعي والمراقبة
والسلطة الرقمية في فلسطين وما بعدها
“



أصوات أسيرة: التجسس الصوتي الخوارزمي في فلسطين سارة فتح الله



سارة منظمة 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 المميّنة 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 والبنى التحتية التي تمكّن هذا النظام.

توطئة

بالنسبة للفلسطينيين تحت الاحتلال الإسرائيلي، أصبح الصوت سلاحًا في إحدى أكثر أنظمة التجسس الجماعيّ تطوراً 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 تحكم وسيطرة يسعى إلى احتواء كل قول كدليل أو مبرر محتمل. يكشف هذا التقرير عن بنية التجسس الصوتي الخوارزمية في فلسطين، ويكشف كيف تحوّل فعل الحديث إلى سلاح رقمي بأيدي الاحتلال.

أهمية التجسس الصوتي

وُصف نظام التجسس الصوتي في إسرائيل بأنه «واحد من أكبر مجموعات بيانات التجسس في العالم وأكثرها تطفلاً 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 وفعلاً، 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 التعرف على الوجه³ 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 والجاهيري. 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 شرطة وحكومة 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»، Magazine، 6 +972 آب / أغسطس 2025، <https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure>.

2 حملة، تكتيق 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 جودفريد، 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](https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf)؛ حملة، تقنية التعرف 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 إباد برغوثي وأليسون كرم، 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 الفلسطيني والمشاركة السياسية عبر شبكات التواصل الاجتماعي (حملة، المركز العربي لتطوير الإعلام الاجتماعي، 2019)، <https://7amleh.org/wp-content/uploads/10/2019>؛ استطلاع-حملة-1.pdf.

5 دانيال لافور، «التجسس الصوتي: 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://sleff.org/technologies/gunshot-detection>.

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

وبشكل أكثر تحديدًا، يركز هذا التقرير على التجسس الصوتي: 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 المعتبرة (في أعمال أحمد ح. سعدي⁸، إيليا زريق⁹ وآخرين¹⁰) تناول السياق المذكور.

المنهجية

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

نظرًا للتعقيد شبه المطلق المحيط 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 متكيفة للندرة أو للشح»¹¹، مما يستدعي الحيلة والاقتدار بمواجهة المعلومات المحجوبة أو المتستر عليها.¹² لا يدعي هذا التقرير أنه يقدم الصورة الكاملة لهيكلية أو مبنى التجسس الصوتي في إسرائيل. عوضًا عن ذلك، فإنه يوفر إعادة بناء حيوية وإن كانت جزئية، حيث تجمع قطع اللغز المتاحة، 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»؟»، 4، The Guardian (New York)، 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: 10 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 الصوتي الإسرائيلي بمعزل عن سياقه التاريخي والنظام البيئي الأوسع للاحتلال القائم على تقنيات التجسس. تكشف هذه القاعدة التاريخية والتحليلية كيف أن التجسس الصوتي لا يعمل كبرنامج تكنولوجي معزول، بل كجزء لا يتجزأ من نظام شامل للتحكم في السكان.

الجدور 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 لاحقاً بالاسم الرسمي «استخبارات الإشارات» (Signals Intelligence) - التنصت على الأسلاك والتشفير وفك التشفير والمراقبة الإلكترونية - كان مضمناً 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 وناثق سلطات الانتداب البريطاني التي تُفصل 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 حالياً مثل الشاباك، جهاز الأمن الداخلي الإسرائيلي الواقع تحت إشراف رئيس الوزراء المباشرة، 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 نطاقاً على صعيد المجتمع ككل.

ترسنة 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، المراقبة والتتبع عن بُعد والمراقبة المباشرة، المنشآت والأسس المتباينة، رسم الخرائط، مسوحات الأراضي وسجلاتها وتطويها، التخطيط الحضري، هندسة العمارة، أبراج المراقبة، السجلات السكانية، الإحصاءات السكانية المجتمعية، بطاقات التعريف والهويات الشخصية، وأدوات أحدث قليلاً بتقنيات غير متطورة، مثل الاعتراض البريدي، والتنصت على المكالمات الهاتفية، وأجهزة الأشعة السينية»¹⁸ وعلى الرغم من أن إسرائيل اعتمدت بشكل متزايد تقنيات تجسس حديثة - كالتطائرات المسيّرة، طائرات بدون طيار، الإنساليات (روبوتات) المُتحكم بها عن بُعد، جمع البيانات البيومترية، والفيروسات الحاسوبية - إلا أن هذه الأدوات «لا تحل محل الأدوات ذات التقنية غير المتطورة، 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.

توثق 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 الإلكترونية 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 المسيّرة، والإشراف على المحتوى الرقمي في شبكات التواصل الاجتماعية وغيرها من الأنشطة عبر الإنترنت، السيطرة على التنقل ومراجعة الهويات، شبكات المُخبرين والمُتعاونين البشريين، وغيرها المزيد.²¹

يجب فهم التجسس الصوتي، على الرغم من كونه المحوّر الوحيد لهذا التقرير، على أنه أحد مركبات نظام بيئي تجسسي مترابط. لا يعمل التجسس الصوتي في عزلة ولكنه يُضخّم بفضل أساليب التجسس الأخرى ويُضخّمها. 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 التعرف على الوجه للمقارنة المرجعية مع البصمات الصوتية بهدف إنشاء ملفات تعريف بيومترية أكثر شمولاً. يخلق هذا الترابط نظاماً 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 الصوتي

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

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

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

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

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

هويات الأفراد المشاركين في محادثة هاتفية والتعرف عليهم،²² يُشير الحجم الهائل للبيانات الصوتية المجموعة حتى الوقت الراهن، إلى اعتماد إسرائيل المحتمل على تعلم الآلة والأدوات الخوارزمية، وليس فقط على التعرف 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 تعلم 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 المتطور. رغم أنهم لم يذكروا الأدوات الدقيقة، أشار باحثو التجسس إيليا زريق ودافيد ليون إلى الصلاحيات الشاملة المعنية بالمراقبة الممنوحة للشاباك والشرطة خلال جائحة كوفيد-19.²⁵ 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 صوته. في مقال لرويتزر يتناول دراسة اختبار صوت أثناء جائحة كوفيد-19 - أجرتها وزارة الأمن الإسرائيلية، أكد المقال على أنه تم تحليل عيّينات من أصوات المرضى باستخدام خوارزميات التعلم الآلي المصممة لتحديد العلامات الصوتية الفريدة وتحديد «بصمة صوتية» للتشخيص والمراقبة عن بُعد. تُوضح الدراسة، أن إسرائيل تملك القدرة التقنية على إجراء تحليل صوتي خوارزمي واسع النطاق دون علاقة بالعمليات الاستخباراتية.²⁸ تساعد هذه السوابق في موضوعة البنية التحتية الحالية لمعالجة الصوت والتسجيلات التي يتم اعتراضها. مما يوفر سياقًا مهمًا لفهم الأدوات التي من المحتمل أن تستخدمها إسرائيل لتحليل بيانات التجسس الصوتي 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 قياض 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، تننيهاه 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 رويتزر، «وزارة الأمن الإسرائيلية تطلق دراسة اختبار صوت كوفيد-19»، رويتزر (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 إتصاليًا».³¹

لم تفلح معاهدات أو سلو عام 1993 بتغيير هذه الظروف للأحسن. في حينه، أقل من 2% من الأسر الفلسطينية كانت تملك خط هاتف أرضي، في حين تملك 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 المعوقات والقيود البيروقراطية 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 مباشرة».³² تعيق هذه التبعية 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 الفلسطينية - عمدًا. تسببت هذه الهجمات، مُجمعة بقدرة إسرائيل 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.2012.41.2.27>.

35 صوفي فلينسبورغ وسيغني سوفوس لاي، «اتباع 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 الصوتي. 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 المعدات التي يجب أن تمر عبر الجمارك الإسرائيلية أو أن تُقتنى من موردين إسرائيليين، 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 مقومات 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 حميمة - الأسرة والعائلة».⁴¹ يخاطب الباحثون الفلسطينيون مدى يومية⁴² ودنيوية⁴³ تقنيات التجسس الخبيثة، من حيث أنها تسمح «بالنسل إلى المنازل واختراق الاتصالات».⁴⁴ يُعتبر التجسس الصوتي، الذي يلتقط المحادثات بين أفراد الأسرة الواحدة والأقارب والمحبيين داخل منازلهم ومجتمعاتهم، واحدة من أوضح التعديات على هذه المساحات العلائقية.

تحمل الطبيعة الانتهاكية للتجسس الصوتي أصداء حميمة داخل حياة الفلسطينيين الخاصة ومجتمعاتهم. وصف الجنود الإسرائيليون المُسرحون من الخدمة، حجم ونطاق التنصت على المحادثات الخاصة أو الحميمة، مُشيرين إلى ما يمكن وصفه بأنه «لا قيود على ما يستطيع الجنود فعله بالمحادثات التي اعتراضوها».⁴⁵ وأضاف أن «الجنود يقومون بحفظ المحادثات وإرسالها إلى أصدقائهم»، في إشارة إلى تنفيه والتقليل من شأن الخصوصية في صفوف أصحاب القدرة على الوصول لبيانات التجسس الصوتي. يتماشى هذا مع مشروع التجسس الصوتي 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 الأصليين والاستعمار الاستيطاني بعد إيليا زريق، محرر: أحمد ح. سعدي ونور مصالحة (I.B. Tauris، 2023)، 188.

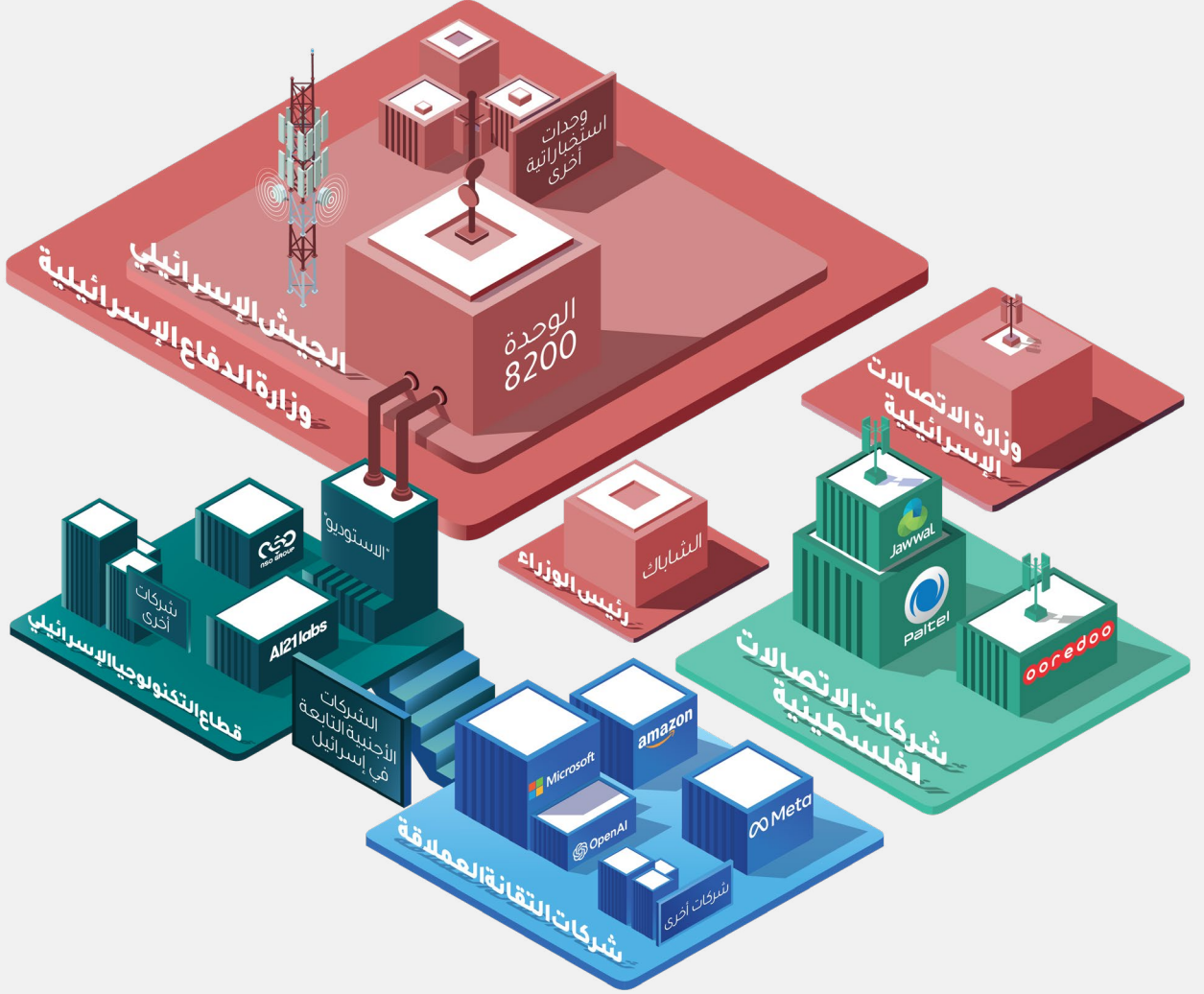
42 Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear, 1st edn (Cambridge University Press, 2015), 27, <https://doi.org/10.1017/CBO9781316159927>.

43 زريق، المشروع الاستعماري الإسرائيلي 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](https://doi.org/10.1016/S0140-6736(12)61280-X).

45 أُلبنى 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 الراخين تحت الاحتلال.



1.2. الجهات المتورطة في التجسس الصوتي

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

الحكومة والجيش الإسرائيلي

في صميم بنية التجسس الصوتي 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،

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 الصوتي.

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 تعزز قدرات التجسس العسكري الإسرائيلي 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 فردية خاصة بإسرائيل، على الأقل جهة فاعلة واحدة في التجسس الصوتي، و 15 جهة فاعلة في المتابعة والمراقبة الهاتفية، إلى جانب أكثر من اثني عشر جهة أخرى فاعلة في التقنيات

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

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

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

Xavier Stephane Decoster et al., The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development, 50 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 الصوتي، 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 ضرورتها في البنية التقنية والعملياتية لمشروع التجسس الصوتي الإسرائيلي.

شركات الاتصالات الفلسطينية

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

1.3. تتبع البيانات (التجسس الصوتي)

بعد أن قمنا برسم خارطة الجهات الفاعلة المعنية، تستدعي الخطوة التالية لفهم منظومة التجسس الصوتي الإسرائيلية 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 إنفستيجيت، «Amazon.Com Inc»، لجنة أصدقاء الخدمة الأمريكيين، 7 آب / أغسطس 2024، <https://investigate.info/company/amazon>؛ إنفستيجيت، «Microsoft corp»، لجنة أصدقاء الخدمة الأمريكيين، 29 كانون الثاني / يناير 2005، <https://investigate.info/company/microsoft>.

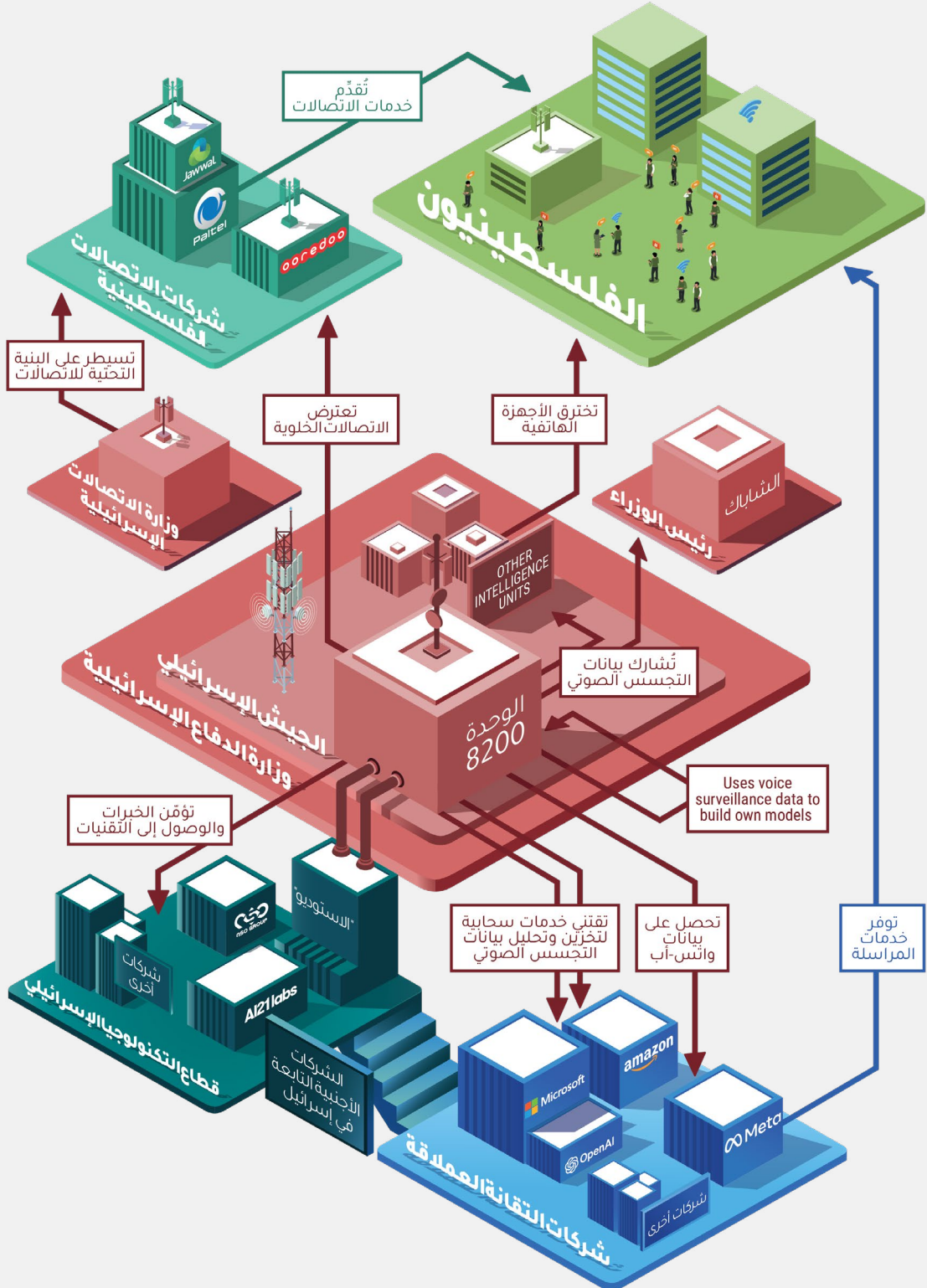
58 داني أوبراين وجيليان سي. يورك، «سفينة بطيئة نحو البيانات السريعة: لماذا لا تزال فلسطين تنتظر 3G؟»، مؤسسة الطليعة الالكترونية، 11 تشرين الثاني / نوفمبر 2015، <https://www.eff.org/deeplinks/2015/11/palestine-3g>.

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.

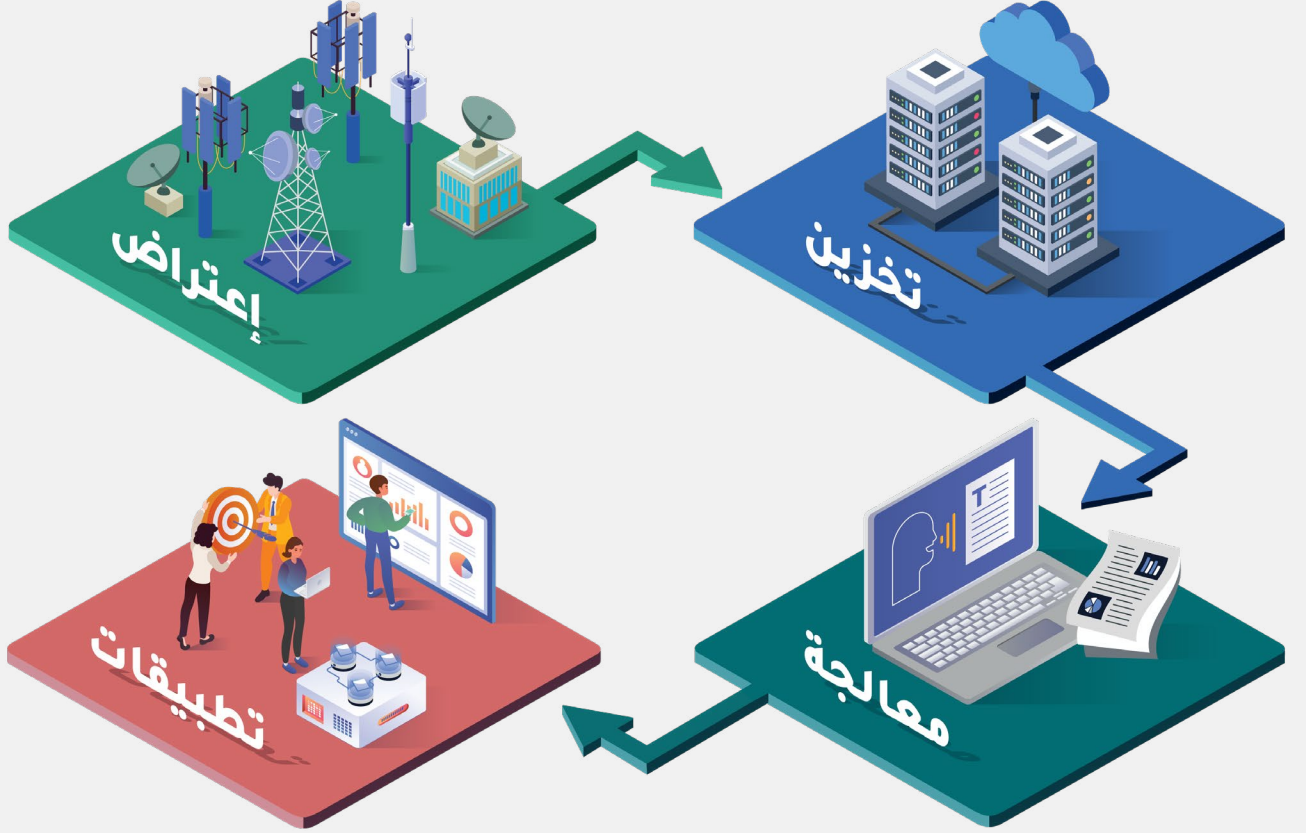
60 فلينسبورغ ولاي، «اتباع البيانات! إستراتيجية لتتبع قوى البنية التحتية»، 319.

61 فلينسبورغ ولاي، «اتباع البيانات! إستراتيجية 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 تفصيلاً في الأقسام التالية.



تتبع بيانات التجسس الصوتي، يُبنى هذا التقرير على أربع خطوات: إعتراض الاتصالات والتقاط البيانات الصوتية (القسم 2)، تخزين بيانات التجسس الصوتي (القسم 4)، معالجة وتحليل بيانات التجسس الصوتي (القسم 3)، وتطبيقات بيانات التجسس الصوتي (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 الصوتي

ما بدأ كمراقبة تستهدف أفراد مُحددin قد توسع إلى نظام تجسس صوتي على مستوى مجتمع كامل. يصف هذا القسم النطاق الحالي للتجسس الصوتي في فلسطين، والمجموعات التي تستفرد بها للتدقيق المُشدد، ونطاقها الجغرافي الآخذ بالاتساع.

تجسس جماعي على كل فلسطيني

يبلغ نطاق التجسس الصوتي الإسرائيلي على الفلسطينيين نطاقاً واسعاً، ويستهدف الجميع. وقد أشارت الصحافية بُنى 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 بحث 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 بالـ«عشوائي»، كونه يُتيح «لضباط المخابرات بإعادة تشغيل محتوى مكالمات الفلسطينيين الخلوية، والنقاط 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. تركز 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 النشاط السياسي».⁶⁹

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

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

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

64 وجدي الجعفري، «مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة»، وكالة معا الإخبارية، 20 كانون الأول / ديسمبر 2014، <https://www.maannnews.net/news/748592.html>.

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

66 هاري ديفيز ويوفال أبراهام، «مليون مكالمات 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 مكالمات 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 تطور 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 الشباك 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 الصوتي في البداية على السكان الفلسطينيين في الضفة الغربية. في السنوات الأخيرة، توسعت 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 الصوتي المُستهدف للأفراد إلى التجسس الصوتي على مستوى المجتمع، وتوسعه 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 مكالمات الفلسطينيين يوميًا، في شكل ملفات صوتية - وليس فقط بيانات نصية،⁷⁷ في أرشفة لـ«ملايين مكالمات الفلسطينيين الخلوية يوميًا في غزة والضفة الغربية».⁷⁸ تشكل هذه التسجيلات الصوتية المُعتزضة لُب مخزون التجسس الصوتي.

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

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

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

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

77 يوفال أبراهام، «طلبية من أمازون»: كيف يخزن عمالقة 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 مكالمات 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 مكالمات 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 أُشير في تقرير لصحيفة «الجارديان»: «تتضمن المكالمات الهاتفية التي تم اعتراضها والمرتبطة بملف تعريف شخص ما [...] الوقت الذي اتصل فيه الشخص وأسماء وأرقام الأشخاص المشاركين بالمكالمة».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 الصوتي المُكالمات التقليدية بالاتصالات السلكية واللاسلكية، لتشمل المعلومات المرتبطة بمكالمات 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 الصوتي 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 مؤكدة، تُعنى بالاعتراض المحتمل للبيانات من تطبيقات المراسلة المشفرة أمثال واتس-أب.

79 روبن جيمس، «التجسس الصوتي والبيانات الضخمة»، 20 Sounding Out!، تشرين الأول / أكتوبر 2014، <https://soundstudiesblog.com/2014/10/20/the-> [/acoustic-era-of-surveillance/](https://acoustic-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-737bc17af7b03e98c2>، 9cec4e15d0f108.

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

82 صدى سوشال، تدعو صدى سوشال 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-lsryb-myta-byanat-mstkhdm-y-oatsab-l-alysh-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 والخزّامي (اللاندر)، 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 الصوتي 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) إسرائيلي مُبرمج».⁸³ يشير استخدام مصطلح «مُضمّن/يحتوي» إلى آلية قائمة على الأجهزة بدلاً 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 أيضاً اختراق الهواتف من خلال برامج التجسس، والتي يمكنها تنشيط ميكروفون الجهاز سرّاً 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 ديفنדרز».⁸⁶ وفي وقت لاحق وبشكل مستقل راجع «مختبر المواطن» بجامعة تورنتو و«مختبر الأمن» التابع لمنظمة العفو الدولية البحث، اللذان أجريا تحليلاً 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

تتبع 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 قيوداً على شركتي الشبكات الخليوية الفلسطينية، لتجبرهم على استخدام تكنولوجيا الهاتف الخليوي من الإصدارات الأقدم «الأكثر عرضة للاستغلال»، وحظرت الوصول

83 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمات 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/>، <https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders>.

86 فرونت لاين ديفنדרز، الأراضي الفلسطينية المحتلة/إسرائيل: تم اختراق ستة مدافعين فلسطينيين عن حقوق الإنسان باستخدام برامج التجسس Pegasus من مجموعة NSO (فرونت لاين ديفنדרز، 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 مكالمات 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 إسرائيل ستضطر للجوء إلى طرق تجسس تتطلب دورًا فاعلاً أكثر، كاستخدام تقنيات تجسس أمثال IMSI (الهوية الدولية لمشاركي الهواتف الخليوية). إلا أنه، بعكس التجسس غير المباشر، 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 مكمويت» 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 لإسرائيل أيضًا.⁹² ومع ذلك، حدّر بيان صحفي 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 إسرائيل 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 أمريكي أمرًا احترازيًا لشركة «ميتا» بمنع برامج NSO التجسسية من استهداف مستخدمي واتس-أب، والصحافيين والمحامين ونشطاء حقوق الإنسان منهم على وجه التحديد، وهو أمر قضائي سعت NSO ناشطة لإلغائه.⁹⁵ 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 الإسرائيلي.

94 مارك أوين [marcwenjones@] جونز، «السؤال حول استخدام لافندر لمجموعات واتس-أب لتوليد أهدافها، ودور ميتا المحتمل في هذا الشأن مهم»، 17 نيسان/أبريل 2024. https://x.com/marcwenjones/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»، 19 Truthout، 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 الصوتي الإسرائيلي 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 المُعتزضة تُستضاف في السحابة، على Microsoft Azure و AWS بالمقام الأول، في حين يُواصل الاحتفاظ ببعض البيانات على خوادم الجيش الإسرائيلي 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 مسربة من مايكروسوفت ومقابلات مع نحو 12 مصدرًا من مايكروسوفت والجيش الإسرائيلي، 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 الصوتي 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 يُخزن عمالقة التكنولوجيا البيانات الجماعية لحرب إسرائيل».

إطار مشروع «نيمبوس» - عقد مُبرم بين جوجل وأمازون والحكومة والجيش الإسرائيليّين، 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 الاستخباراتية عن تقريبًا «الجميع» في غزة.¹⁰⁵ رغم استخدام هذا النظام منذ نهاية عام 2022، إلا أن دوره العمليّاتي قد توسّع بشكل عظيم بعد أكتوبر 2023.¹⁰⁶

الاعتماد على البنية التحتية السحابية لشركات التقنية العملاقة

تقر المصادر العسكرية الإسرائيلية بأن حجم بنية التجسس الصوتيّ الخاصة بها يستلزم الاعتماد على مزودي الخدمات السحابية في شركات التقنية العملاقة، لأنها «كبيرة جدًا بحيث لا يمكن تخزينها على الخوادم العسكرية وحدها».¹⁰⁷ على حد تعبير الضابط المسؤول عن مديرية 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» لـ Azure ضرورية لتخزين اتصالات مجتمع بأكمله، بل أنها كانت تطمح لتوسيع هذه العملية بشكل مُعتبر لتتضاعف «عشرة أضعاف في السنوات القليلة المقبلة».¹⁰⁹

3.2. موقع مراكز البيانات والخوادم

سلّطت أحدث التقارير الضوء على التوزيع الجغرافي للبنية التحتية المستخدمة لتخزين بيانات التجسس الصوتيّ الإسرائيليّ 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 التحول الرقمي»، 8 CIO، 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 ميدنمير 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 مجمل البيانات - مقارنة بالحجم المخزن 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 الصوتي 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 يؤكدته 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 تخزن 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 بنيتهم التحتية لمراكز البيانات التابعة لهما في السنوات القليلة الماضية، حيث دشنت مايكروسوفت مجمعًا لمركز بيانات في إسرائيل عام 2020¹¹⁸

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 لتكنولوجياها في التجسس الجماعي على الفلسطينيين»، ذي جاردان، 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 جاردان، 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 لتكنولوجياها 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 ت دشّن 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 الصوتي داخل إسرائيل.

3.3. فترات الاحتفاظ بالبيانات

لا يزال احتفاظ إسرائيل بالبيانات الصوتية الفلسطينية التي تم اعتراضها مرثًا من الناحية العملية. وفقًا لمصادر استخباراتية في التحقيقات الأخيرة إزاء التخزين في Microsoft Azure، يتم عادة الاحتفاظ بتسجيلات المكالمات - 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 الصوتي المخزنة في Amazon AWS.

4. مُعالجة البيانات الصوتية وتحليلها

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

4.1. التعرف على المُتحدّث

بعبارة مبسطة، من المرجح أن تستند قدرة إسرائيل على التعرف على المشاركين في المكالمات المُعترضة إلى طريقتين واسعتين لتحديد هويّة 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 مكالمات أو تلقيها. من خلال ربط معرف 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 مكالمات في الساعة»: تعتمد إسرائيل على سحابة مايكروسوفت للتجسس واسع النطاق على الفلسطينيين.

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

122 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجياها في التجسس الجماعي على الفلسطينيين».

123 ديفيز وأبراهام، «مليون مكالمات 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 بالمكالمة».¹²⁴

البصمة الصوتية البيومترية

الطريقة الثانية، البصمة الصوتية، هي تقنية بيومترية تستمد توقيعا 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 إسرائيل أن تشتري أو تحصل على الميكروفونات حتى، بالذات تلك المُركّبة بالهواتف الخلوية.

تؤكد العديد من المقالات التعليقية مؤخرًا - وبالأساس مقالات الرأي - أن إسرائيل توظف 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 التنصّت، 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 متسقة، 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 توظف البصمات الصوتية بعد التنصّت على المكالمات الهاتفية وتتبع سجلات مكالمات

124 بيسيكرو وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكي الصنع في الحرب، تتشأ 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>، <https://en.majalla.com/node/310146>.

127 ماركو موساد، «تقنية استنباط البصمة الصوتية: ضربة تجارية ذات فائدة عسكرية»، المجلة، 7 شباط / فبراير 2024، <https://en.majalla.com/node/310146>، <https://en.majalla.com/node/310146>.

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 لتعقب 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، مُضيفاً 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 مزودي التكنولوجيا

من ناحية، يرجح أن تقوم وحدات الاستخبارات الإسرائيلية 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 داخلياً، أو أنه اقتناها من موردين محليين من القطاع الخاص، أو من مزودين دوليين. يشمل القطاع الخاص في إسرائيل عددًا كبيراً من الشركات ذات قدرات التحليل الصوتي المتقدمة، ومن المعروف أن الوحدة 8200 تقوم بتطوير تقنياتها الخاصة. وبالتالي، يظل مصدر أدوات تحديد هُويّة المتحدث سؤالاً يتطلب الجواب.

4.2. تنضيد وتدوين الكلام وترجمته

يتطلب نظام التجسس الصوتي 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 معظم 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 - تتنصّت- المخابرات- الإسرائيلية على-جوالك- الشخصي.

131 هناء صلاح، «البصمة الصوتية أداة إسرائيل 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 الجواله للمقاومة الفلسطينية واللبنانية»، رأي اليوم، 21 حزيران / يونيو 2016، <https://www.raiayoum.com/تفاصيل-مذهلة-عنطرق-وأساليبالمراقبة-ا>

133 AVG، البرمجيات الخبيثة لا تزال تتجسس عليك حتى عندما يكون هاتفك الخلوي مُعطلاً، 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 مكالمات هاتفية في الضفة الغربية وغزة».

135 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمات 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 أصلاً»¹³⁸؟

يشرح خبراء سلاسل التوريد الخوارزمية بأنها جزء من نهج عمل مزوّد الخدمات السحابية. تقدم هذه الشركات، كما هو الحال بالنسبة لمايكروسوفت، تقنيات الذكاء الاصطناعي الخاصة بها التي سبق وُضعت، 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 Translate¹⁴⁴ لبيانات التجسس الصوتي التي تُخزنها على AWS.

136 نكسر الصمت، حُكم عسكري: شهادات جنود من الإدارة المدنية، منشق 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 المساواة 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 الإسرائيلي 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، وفقاً لموقعها الإلكتروني، تحويل الكلام إلى نص، بما في ذلك تدوين الملفات الصوتية المسجلة مسبقاً بالإضافة إلى تدوين بدفعة واحدة لأحجام كبيرة من الملفات الصوتية.¹⁴⁸ وتشمل خصائص إضافية ذات صلة تحديد اللغة، تقييم النطق، وترجمة الكلام.¹⁴⁹ نظراً 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 الصوتي الإسرائيلي على استخدام تحليل الكلام؛ علماً 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 لأجراء 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 الصوتي.¹⁵¹

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

145 بيسيكرو وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تتشأ 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 بيسيكرو وآخرون، «بينما تستخدم إسرائيل موديلات ذكاء اصطناعي أمريكية الصنع في الحرب، تتشأ 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 المحددة 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 التدريب 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 يُمكن 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 تطويرها 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 تتوفّر 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 بيسيكرو 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 يُخزن 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 الإسرائيلي على الولوج من منصة Azure بدلاً من الولوج مباشرة 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 المزود بالتحديد، بدلاً من الولوج إليها من خلال منافس».¹⁶⁵

تتيح العمليات والتقنيات الموضحة أعلاه التعرّف على البيانات الصوتية، تدوينها، ترجمتها، مُعالجتها، وتحليلها على نطاق واسع. بمجرد 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 كمواضيع 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 العملية. حيث ذكرت «ميدل إيست آي» عام 2021 أنه «تتم ترجمة النصوص بعد تدوين المُحادثات وإرسالها إلى وحدات استخبارات الجيش والشبابك».¹⁶⁶ تؤكد تقارير حديثة سير العمل المذكور: يستطيع القادة «الولوج إلى المعلومات الاستخباراتية الأولية المترجمة إلى العبرية».¹⁶⁷ في الممارسة العملية، هذا يعني أن المُحادثات الصوتية المُعترضة - التي يتم تدوين محتواها وترجمته - تُوفّر معلومات استخباراتية خام يتم توزيعها على الجيش الإسرائيلي ووكالات الأمن الداخلي.

161 أبراهام، «وثائق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».

162 أبراهام، «وثائق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».

163 أبراهام، «وثائق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».

164 أبراهام، «وثائق مُسرّبة تكشف علاقات وثيقة بين الجيش الإسرائيلي ومايكروسوفت».

165 كوب وآخرون، «فهم المسألة في سلاسل التوريد الخوارزمية»، 1191.

166 مصاروة، «مصدر استخباراتي: تستطيع إسرائيل مراقبة أي مكالمات 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 الصوتي مع بيانات أخرى محدودة، لكن المصادر المُتوفرة تشير إلى أنها تشكل جزءًا من مجموعة أوسع من قواعد البيانات. يَرجح أن يكون يوسي سارثيل، الرئيس السابق للوحدة 8200 والمهندس الرئيس لاستراتيجية الذكاء الاصطناعي، «قاد مشروعًا واسع النطاق وذي تمويل مُعتبر، وسَّع 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 يشرح من كتابات سارثيل اجراء تقاطع مرجعي لـ «المعلومات المرئية، البيانات الخلوية، جهات اتصال وسائل التواصل الاجتماعي، صور، وجهات اتصال الهاتف الخليوي»، وربما أكثر من ذلك،¹⁶⁹ مرددًا توصيف إيليا زريق لطبقات إسرائيل من جمع بيانات التجسس الجماعي.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 الصوتي أيضًا كمواود 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»، 12-13.

171 بيسيكرو 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 بيسيكرو 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 فريكل 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

وفقاً 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 نظراً «لقدرتها على تجميع بيانات موزعة في مصادر متعددة. عوضاً عن استخدام «أدوات البحث البدائية»، يستطيع الضباط بكل بساطة «طرح أسئلة وتلقي إجابات» من بوت المُحادثة».¹⁷⁸ يمكن الاستعلام عن بوت المُحادثة، 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 الصوتي لهذا النموذج اللغوي الكبير عوضاً 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 غالباً ما يجري تدريب النماذج العربية التجارية أو مفتوحة المصدر الحالية على اللغة العربية الفصحى، وليس اللهجات المنطوقة التي يستخدمها الفلسطينيون بالحياة اليومية. لذلك جمعت الوحدة 8200 «جميع النصوص (العربية المنطوقة) المُدونة التي تملكها الوحدة» وأدخلتها في مستودع مركزي لاستخدامها كمجموعة بيانات تدريبية.¹⁸³ وبحسب مصادر تحدثت لصحيفة «ذي جاردريان»، 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 قيمة 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 الصوتي 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- أوش، «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 الصوتي 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 للتحضير لغارات جوية مُميتة في غزة.¹⁸⁸ كما كشفت «ذي جارديان» أنه تم استخدام «المخزون العائل من المكالمات الهاتفية» المُخزنة في Azure لتحديد أهداف القصف.¹⁸⁹

تبعًا لمؤلفاتهما التي تناولت العنف اليومي للتجسس الإسرائيلي، توضح شلهوب - كيفوريان 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، تُسمي 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 الصوتي 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 المُبلغ عنها في نظام

185 يوفال أبراهام، «لافندر»: جهاز الذكاء الاصطناعي الذي يوجه 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 تُخزن 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 - كيفوريان وعثمان، «السرية كعنف استعماري: حالة القدس الشرقية المحتلة»، 191.

191 سارة فتح الله، «الذكاء الاصطناعي والتحكم 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 الصوتي 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 تبين أن معدلات دقة التعرف المؤتمت على الكلام باللغة العربية دون المستوى.¹⁹⁴ تباين اللهجات واللكنات ومخارج الحروف تؤدي إلى مضاعفات إضافية¹⁹⁵ 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 يكشف الضباط الناطقون بالعربية بعض الأخطاء،¹⁹⁷ إلا أن التحيز التأكيدي¹⁹⁸ والعمل المُضاف¹⁹⁹ 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» - مخرجات 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 توظفها، تزيّف وتختلق النصوص، إلى جانب كونها «تُضيف تعليقات عنصرية وتستخدم خطأً عنيفاً».²⁰¹ تعترف المصادر بأن «الاعتماد الأعمى على هذه الأدوات» مُحتمل،²⁰² مما يزيد من خطر تأثر القرارات بمعلومات مُختلفة حقيقة.

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

192 بيسيكرو 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، «سير القياسات الصوتية البيومترية: مقارنة وتباين كيف تقوم الدولة والقطاع الخاص بتحديد الهوية من خلال الصوت»، البيانات الكبيرة والمجتمع 11، رقم 4 (2024): 20539517241297889. <https://doi.org/10.1177/20539517241297889>

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

197 بيسيكرو 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 بيسيكرو 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 بيسيكرو 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 بيسيكرو 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 ماكليين، «أليكسا، هل أنا سعيد؟ كيف يُحقق التعرف 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 الهوية البيومترية واستدلال العواطف والنوايا.

تُفاقم هذه المخرجات بفعل كون بعض هذه الأدوات تعمل كـ«صناديق سوداء»، إلى جانب معرفة محدودة بكيفية توليد الأنظمة الخوارزمية للمخرجات أو تقديم التوصيات، مما يمنع إمكانية تتبع كيفية الوصول إلى الاستنتاجات أو تصحيح الأخطاء. وبالرغم من ذلك، قد لا تكتثر إسرائيل أصلاً لتقليل معدلات الخطأ، إذ ذكرت مصادر إسرائيلية أن «القضية الأكثر إلحاحاً 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 الصوتي الإسرائيلي آثار عميقة على الفلسطينيين، إذ أنه يصوغ ويبرمج الحياة اليومية من خلال الاتهام، التجريم، والعواقب المميّنة. وتبقى هذه التأثيرات والعواقب مرتبطة بالسياق العسكري والقتالي الأوسع للاحتلال.

الاتهام والاعتقالات

تسهل بيانات التجسس الصوتي بشكل مباشر اعتقال الفلسطينيين. يُتيح النطاق المتسع للتجسس المُعزز بقواعد البيانات الصوتية الضخمة التابعة للوحدة 8200، للقادة العسكريين تجميع قوائم كبيرة من المُشتبهين في جميع أنحاء البلدات الفلسطينية، مما يُسهّم 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 شهرياً في منطقته»، حسبما كشف أحد المصادر.²⁰⁷ إن الحد الأدنى المنخفض جداً للاشتباه بالشخص - غالباً ما يكون غامضاً أو غير مدعوم بأدلة - يُتيح للسلطات الإسرائيلية تبرير الاحتجاز، الابتزاز، أو حتى القتل المستهدف بأثر رجعي، باستخدام البيانات الصوتية لإضفاء الشرعية على قراراتها. فكما أكد مصدر لصحيفة «ذي جاردريان»: «عند حاجتهم باعتقال شخص من دون توفّر سبب وجيه للقيام بذلك، هذا هو المكان الذي يجدون فيه المُبرر»، في إشارة إلى بيانات التجسس الصوتي المخزنة على السحابة.²⁰⁸ يُتوقع 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 مناهجاً من الرُعب والرقابة الذاتية.²¹⁰ «لإدراكهم أن ما يقولونه [...] قد يكون مُراقباً 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 بالسكان»، 16.

الوقت»²¹¹، يمتنع الفلسطينيون عن التعبير السياسي أو يتجنبون التحدث بحرية كما يحلو لهم،²¹² إذ أنهم يتوقعون احتمال أن تُوظف مُحادثاتهم كمواحد 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 ويُضيق 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 الصوتي 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 والاعتقالات

كما يمكن ربط التجسس الصوتي مباشرة بالحصائل الدامية والمُمتنة. إذا ما كان التجسس الصوتي يُوظف فعلاً كمُدخلات لأنظمة توليد الأهداف المؤتمتة التابعة للجيش الإسرائيلي، ستكون هذه التداعيات كارثية أكثر بكثير.²¹⁷ أحد الأمثلة المأساوية التي أوردتها «لوس أنجيليس تايمز» هي حالة جمانة، أم فلسطينية استشهدت في غارة جوية إسرائيلية مع توأمها البالغين من العمر 4 أيام في غزة، حيث يشتبه أفراد أسرتها وزملاؤها في أنها استهدفت خطأ باستخدام الذكاء الاصطناعي وبيانات الهاتف. وقد قال صديق للعائلة: «لا مبرر. بالمرّة»، مضيّقاً 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 والمُمت، المخاطر والعواقب الجسيمة للتجسس الصوتي على الفلسطينيين، مما يجعل مقاومة هذه المنظومة والاعتراض عليها أكثر إلحاحًا.

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

212 أسيد 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 جودفريد، «عندما يُشكّل حديث فلسطيني عن السياسة تحريضاً»، Jewish Currents، 15 أيلول/ سبتمبر 2021، <https://jewishcurrents.org/when-palestinian-political-speech-is-incitement>.

214 جودفريد، 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، «مُراقب، مُتابع، ومُستهدف».

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 أنجيليس تايمز، 14 آب/ أغسطس 2024، <https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike>.

8. السُّبُل المُحتملة للاعتراض

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

8.1. المُحاسبة المُجزأة

عند النظر إلى بنية التجسس الصوتي ككل، يبدو أن العديد من الجهات الفاعلة تعمل بالتنسيق مع بعضها البعض. تشمل الجهات الفاعلة الأساسية في سلسلة توريد التجسس الصوتي 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 بالبنى التحتية الرقمية، إذ أنه، بنظرها، عند تتبع «مسارات التجسس الرقمي» تستطيع أن تدرك كيف «لإسرائيل 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 المُنسقة هو ما يُطلق عليه خبراء التكنولوجيا اسم «مشكلة تعدد الأيدي».²²¹ تنبُع المُشكلة من الحقيقة أنه لا جهة فاعلة تتحرك وحيدة، تتحمل مسؤولية الأفعال التي تُساهم عدة جهات فاعلة فيها بطرائق مُختلفة. وبالتالي، تتوزع 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.

تُعقد السرية والضبابية مهمة استيعاب وتحديد كافة الجهات الفاعلة وأدوارها في سلسلة توريد التجسس الصوتي.²²³ ترفض الوحدات العسكرية الإسرائيلية التعليق أو التعقيب على أفعالها وعملياتها، في حين تدعي شركات النقانة 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 المسألة في سلاسل التوريد الخوارزمية»، 1186.

221 هيلين نيسنبوم، «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 المسألة 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 الصوتي بالذات.²²⁵ وتشير تقارير إلى تطوير شركات إسرائيلية خاصة لأشكال إضافية من التجسس الصوتي، بينها «توكا» (Toka)، الشركة المسؤولة عن تطوير أداة للتنصت 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 هيكلة التجسس الصوتي هذه، وإن لم تكن جميعها معروفة للجمهور.

ومع ذلك، رغم كون العديد من الجهات الفاعلة إحدى مكونات سلسلة التوريد القائمة على البيانات، من الضروري ألا نُنكر أهمية ترتيباتها غير المتناسقة. بعض الجهات الفاعلة، وخاصة الجيش الإسرائيلي ومزودي 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، وتجذب 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 الكبرى بشكل منهجي دورًا أهم في تحمل المسؤولية عن نتائج سلسلة التوريد.²²⁹ تملك شركات التكنولوجيا الكبرى، كونها تزود الخدمات بشكل مباشر كما أسلفنا الذكر في هذا التقرير، كما الشركات المستثمرة، المستحوذة والداعمة للشركات الإسرائيلية المتورطة في بنية إسرائيل للتجسس الصوتي - أمثال، Nvidia، التي تخوض مُحادثات للاستحواذ على AI21 Labs²³⁰ المزيد من القوة في سلسلة التوريد بحكم الأمر الواقع. عند إدانة القوة التي تحملها سلسلة توريد التجسس الصوتي 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 والفاعلين في شؤونها الداخلية

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

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

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

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

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

229 كوب وآخرون، «فهم المسألة 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 الصحفيين والكشف عنها للجمهور، لأجل وضعها رهن التدقيق وتعريض الشركة للمساءلة والضغط؛ ومن بين هذه الأمثلة، يمكن الإشارة إلى الكشف عن استخدام الوحدة 8200 خدمات Azure لتخزين بيانات التجسس الصوتي.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 مُجمعين 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 «لاقتراح انتهاكات لحقوق الإنسان أو انتهاكات للقانون الإنساني الدولي».²³⁴ بعد أن كشفت التحقيقات عن دور الشركة في تخزين كميات طائلة من بيانات التجسس الصوتي 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 أي مخاطر لانتهاكات حقوق الإنسان في بلدان يوجد منها تخوفات 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 وفَعَال.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 المصوّنة.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 لتكنولوجياها 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 تورطها 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»، 3 Truthout، 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»، 9 GeekWire، 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)، مظاهرات 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 2025²³⁸ وثانيها في أيلول/ سبتمبر من العام ذاته²³⁹ - 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 وتوعي الجمهور أيضًا. في الواقع، تعتمد الكثير من المعلومات التي يقدمها هذا التقرير عن بنية التجسس الصوتي 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 الصوتي 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 الصوتي، 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 الصوتي 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، «نشاط في هولندا يحتجون على سطح مبنى تابع لمايكروسوفت تستخدمه لتخزين البيانات العسكرية الإسرائيلية»، ذي جارديان، 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 المفوض السامي لحقوق الإنسان، من اقتصاد الاحتلال إلى اقتصاد الإبادة الجماعية: تقرير المقرر الخاص المعني بحالة حقوق الإنسان في الأراضي الفلسطينية المحتلة منذ عام 1967، A/HRC/59/23 (2025)، <https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur>.

وتقارير صحافية استقصائية.²⁴¹ شكّل هذا القرار سابقة جديدة، حيث أن هذا «الانتهاء 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»، موجهة للمُدير التنفيذي للشركة باقة من الأسئلة: «ما هي الخطوات، إذا ما كانت ستُتخذ، التي ستُتخذها [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». فينظره، 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 الصوقي 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. أثّرت 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 الصوقي المُخزنة 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 لإسرائيل 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 الصوقي إلى مُساءلات واستجابات برلمانية، مما اضطر وزير الخارجية

241 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجياها في التجسس الجماعي على الفلسطينيين».

242 ديفيز وأبراهام، «مايكروسوفت تمنع استخدام إسرائيل لتكنولوجياها 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 قائلاً: «إذا كانت هناك مؤشرات جدية على جرائم جنائية بحسب تلك المعلومات، فيمكن بالطبع بدء اتخاذ إجراءات 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 إسرائيل تجنب وتخفيف المخاوف من مواجهة دعاوى قضائية من خلال الاحتفاظ ببيانات التجسس الصوتي في أطر خاضعة لولايتها القضائية. إذ أن مزودي الخدمات السحابية الرئيسيين أنشأوا مراكز بيانات خاصة بهم في إسرائيل. وقد قال مصدر لمجلة 972+ أنه من شأن هذا الأمر تذييل المخاوف من إجراءات قانونية في محاكم الخارج.²⁵⁰ هذا التكتيك شائع في سلاسل التوريد الخوارزمية، حيث تستخدم الجهات الفاعلة أي «استراتيجية تقنية قانونية» تساعد على تقليل المخاطر، وفي حالة سلاسل التوريد العابرة للحدود، فهي تستفيد من المراجعة التنظيمية.²⁵¹ كما تستطيع إسرائيل أن تطلب التعاون من شركات التكنولوجيا، إذ تنص العقود مع شركات أمازون 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 لإسرائيل نقل بياناتها على جناح السرعة، كما كان الحال في شأن البيانات التي خزنتها 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 الصوتي خرقًا للقوانين المحلية الأجنبية، وكذلك للقانون الدولي. وبصفتها ائلاً 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 لتورطها 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 حد كبير، قابل للمحاكمة في المحاكم المحلية في الولايات المتحدة والاتحاد الأوروبي، وأمام مختلف الهيئات الدولية»²⁵⁵ كمحاكمة الجنايات الدولية.

248 ديفيز، «نشاط في هولندا يحتجون على سطح موقع لمايكروسوفت يُستخدم لتخزين البيانات العسكرية الإسرائيلية».

249 أوكارول، «مطالبة السلطات الأيرلندية التحقيق مع مايكروسوفت إزاء معالجة مزعومة غير قانونية للبيانات من قبل الجيش الإسرائيلي».

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

251 كوب وآخرون، «فهم المسألة في سلاسل التوريد الخوارزمية»، 1194-95.

252 هاري ديفيز ويوفال أبراهام، «كشف: إسرائيل طالبت غوغل وأمازون باستخدام «غزوة» 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 لتكنولوجياها في التجسس الجماعي على الفلسطينيين».

254 أوكارول، «مطالبة السلطات الأيرلندية التحقيق مع مايكروسوفت إزاء معالجة مزعومة غير قانونية للبيانات من قبل الجيش الإسرائيلي».

255 مركز القانون المناهض للعبودية، «دور مايكروسوفت المُساند للإبادة الجماعية التي ترتكها إسرائيل ضد الفلسطينيين تعرض الشركة وقيادتها للمساءلة القانونية»، مركز القانون المناهض للعبودية، 2 كانون الأول / ديسمبر 2025.

تستطيع الدول التي تعترف باختصاص وصلاحيات 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 يُوفّر القانون الإنساني الدولي وقانون حقوق الإنسان سُبُلًا 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 أوصلو، 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 تُمكن انتهاكات حقوق الإنسان في القائمة السوداء، كالشركات المتورطة في منظومة التجسس الصوتي 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 الصوتي، 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 الصوتي 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 المُنسقة للطعن على أنشطتها، إلا أن المطالبات 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 - توفّر مسارات لتعطيل الأنظمة التي تمكن التجسس الصوتي الخوارزمي الإسرائيلي على الفلسطينيين.

256 ريان جريم ووقاس أحمد، «وثائق مُسرّبة: الجيش الإسرائيلي هو واحد من أفضل عملاء مايكروسوفت في شأن الذكاء الاصطناعي»، 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 المُقيد المقيد لتنمية فلسطين.

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

260 هانا كيللي، «التكنولوجيا مزدوجة الاستخدام وضوابط الصادرات الأمريكية، مختبر سياسة تكنولوجيا 15 CNAS، حزيران / يونيو 2023، <https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls>.

الخلاصة

يستعرض تقرير «أصوات أسيرة» الانتهاك العميق الكامن في قلب التجسس الصوتي الإسرائيلي الخوارزمي الجماعي. الاستيلاء المنهجي على كلام ومُحادثات الفلسطينيين كآلية لقمعهم. أظهرت الفصول السابقة أن منظومة التجسس الصوتي المُطبقة على الفلسطينيين لا تعمل في فراغ وليست برنامجًا منفصلاً أو معزولاً، وببل 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 الصوتي 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 الصوتي المنهجي للفلسطينيين عن حجم الاحتلال العسكري الإسرائيلي فحسب، بل يكشف أيضاً عن الدور المحوري للشركات وشركات التكنولوجيا ومقدمي الخدمات السحابية، الذين يمكن الضغط عليهم جميعاً 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 أيضاً التصدي للعقلية الاستعمارية والمنطق السرطاني التوسعي الذي جعل مثل هذه المنظومة أصلاً قابلة للتصور والتطبيق. دون معالجة هذه الهياكل الأساسية - بما في ذلك تطبيع التجسس الجماعي 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 إلغائه مفعوله.

ربما الوقائع المعروضة هنا ليست إلا غيض من فيض أو لمحة عن منظومة التجسس الصوتي الأكبر والأكثر غموضاً، 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-Filistīniyīn Wa-Lmušārka Ās-Syāsyā ‘abra Šabakāt at-Ttawāṣul ā-L’ijtimā’y [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/2019-10/استطلاع-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-Āhtilāl Yastħdim Bašma’ al-Šūt Wāl’īn Lit’qwb Muqātilī al-Muqāwama Biġaza [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/2025-الصوت-بصمة-الاحتلال-يستخدم-الصوت-والعين-لتعقب-مقاتلي-المقاومة-بغزة-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](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 Kivalova. '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, Ihab 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/2025/04/25/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/10.4324/9780203845967/>.
- 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/2024/10/09/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/2021/08/11/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/2014/20/10/the-acousmatic-era-of-surveillance/>.
- Jamil, Yassin. "'Tafāṣīl Muḍhila 'an Ṭuruq Wa 'asālib al-Murāqaba as-Sirrya al-Isrā'īliya Lil-Hawātif al-Jawwāla Lil-Muqāwama al-Filṣṭīniya Wal-Lubnāniya" [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/ا-أساليب-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/10.1177/20539517241297889/>.
- 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%9s-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 ālmuḥābarāt āl'isrā'īliya 'alā jawwālik āṣaḥsy!?" كيف تتنصت المخابرات الإسرائيلية؟ [How does Israeli intelligence eavesdrop on your personal mobile phone?!]. Palestine Today, 30 December 2013. <https://paltodaytv.com/post/466/على-جوالك-الشخصي-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-aaggl-ofory-ltsryb-myta-byanat-mstkhdm-yatsab-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 Litanfīd 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/2023/5//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/2011/9/11//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.l68.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/59/2025.23/. <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/10.4324/9780203845967/>.

- 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

تواصلوا معنا:

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

صفحاتنا على وسائل التواصل الاجتماعي: 7amleh

