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

صناعة أنظمة المراقبّة الإسرائيليّة وحقوق الإنسان:

آثارها على الفلسطينيين وتداعياتها في العالم

كانون الأول/ديسمبر 2023

حملة - المركز العربي لتطوير الإعلام الاجتماعي

كانون الأول / ديسمبر 2023

صناعة أنظمة المراقبّة الإسرائيليّة وحقوق الإنسان:
آثارها على الفلسطينيين وتداعياتها في العالم

نطلّع لتواصلكم/ن معنا عبر القنوات التّالية:

البريد الإلكتروني: info@7amleh.org

الموقع الإلكتروني: www.7amleh.org

هاتف: 20670 7740 (0) 972 +

تابعونا عبر صفحاتنا على منصّات التّواصل االجتماعيّ: 7amleh

مقدّمة

يقدّم هذا التّقرير لمحةً عامّة عن واقع صناعة أنظمة المراقبة الإسرائيليّة، متعقّبًا آثارها على حقوق الإنسان للشعب الفلسطيني وتداعياتها الحقوقيّة على صعيد العالم أجمع. يستند التّقرير في تحليله إلى الأدبيّات الأكاديميّة، والموجزات السّياساتيّة، والبحوث السّابقة حول الواقع الفلسطينيّ في ظلّ ما يشهده من مراقبةٍ حكوميّةٍ مكثّفةٍ في الضّفّة الغربيّة بما فيها القدس الشّرقيّة. في معرض أقسامه الخمسة، يُضيء التّقرير على سياق نمو صناعة أنظمة المراقبة الإسرائيليّة بالتّوازي مع التّوجّهات العالميّة على صعيدَي الأمننة والمراقبة مع بداية القرن الحادي والعشرين، كما يتطرّق لأثر برمجيّات التّجسّس، ورصد وسائل التّواصل الاجتماعي ومراقبتها، عدا المراقبة البيومتريّة، وذلك في الداخل والأرض الفلسطينية المحتلة عام 1967 والعالم عامّةً. خِتامًا، يقدّم التّقرير جُملةً من التّوصيات الرّاميّة للتخفيف من الآثار الضّارة لهذه الأنظمة. تصاعدت واستشرست ممارسات المراقبة الإسرائيليةبحقّ الفلسطينيين/ات في المنطقة على نحوٍ ملحوظ مُنذ السّابع من تشرين الأوّل/أكتوبر ومع تواصل الحرب الإسرائيليّة على قطاع غزّة، ومع تكثيف التّكتيكات الأمنيّة والعسكريّة في خضمّ الأيّام القليلة الماضيّة، أطلقت تدابير الطّوارئ عنان صلاحيّات المراقبة الممنوحة لجهاز الشّرطة وآلة الحرب الإسرائيليّة على الفلسطينيين/ات في الداخل والأرض الفلسطينية المحتلة عام 1967. يوفّر هذا التّقرير من خلال تسليطه الضّوء على التّاريخ الحديث لصناعة أنظمة المراقبة الخاصّة الإسرائيليّة وآثارها وظلالها على الفلسطينيين عموماً والضّفّة الغربيّة بما فيها القدس الشّرقيّة خصوصاً سياقًا تتجلّى فيه، أي هذا السّياق، جذورَ وحيثيّاتِ الأحداث الرّاهنة.

تطوّرت الابتكارات أولًا في مجال المراقبة الرّقمية ثُم المراقبة الآليّة (المؤتمتة) وعملت على توسيع نطاق المراقبة الإسرائيليّة على الفلسطينيين مع مطلع القرن الحادي والعشرين. أسهم الكثير من هذه التّقنيات الّتي طوّرت ونُقّحت في فلسطين في نمو صناعة الأمن القوميّ العالميّة الّتي تُعلي من شأن ابتكارات المراقبة الرّقميّة والآليّة. تُظهر دراسات الحالات الثّلاثة فيما سيأتي من هذا التّقرير كيف آلَ استخدام تقنيات المراقبة التّوغّليّة على الفلسطينيين/ات إلى تمكين الشركات الإسرائيليّة تصدّر مشهد هذه الصّناعة الخاصّة، مصدّرةً أنظمتها التّوغّليّة لمختلف أرجاء العالم. تُوضح هذه الأمثلة الأثر القمعي لأنظمة المراقبة الجديدة على حياة المدنيين الّذين يرزحون تحت رقابة أمنيّة مكثّفة أو احتلالٍ عسكري. تتسبّب الأنظمة التي تم التطرق لها في هذا التّقرير على مفاقمة العنف و الإجحاف بحقوق الإنسان في فلسطين. يوضّح التقرير أيضًا كيف أسفرت تقنيّات المراقبة الجديدة إلى تآكل الحق الأساسي للفلسطينيين/ات في الخصوصيّة، فضلًا عن حقّهم في الحركة والتّجمّع، عدا عن حرّيّة التّعبير، كما نصَّ عليه الإعلان العالمي لحقوق الإنسان.[1] في ضوء فهم آثار تقنيّات المراقبة الجديدة في الأرض الفلسطينية المحتلة عام 1967 وتداعياتها العالميّة، يُشدّد هذا الموجز السياساتي على الحاجة لكبح جماح هذه الأنظمة—بما في ذلك الكف عن تطويرها ونشرها وتصديرها.

ثانيًا. سياق

تمتدّ جذور تاريخ عسكرة المراقبة الإسرائيليّة للفلسطينيين/ات لما قبل عام 1948، ذاك العام الّذي شهد على تهجير 750000 فلسطيني/ة من ديارهم، فيما أُخضِع من بَقَوْا لِحكم عسكريٍّ إسرائيليٍّ كانت المراقبة الشّاملة أبرز سِماتِه.[2] كما يشير المؤرخون/ات الفلسطينيون/ات، فإنّ ضم إسرائيل واحتلالها اللّاحق للأرض الفلسطينيّة (قطاع غزّة والضّفّة الغربيّة بما فيها القدس الشّرقيّة) عام 1967 قد مدّ ظلال هذه الممارسات لتتجاوز خط الهدنة لعام 1949.[3] لعقود، أسفر التّجسّس الإسرائيلي، والتنصّت، والاستطلاع الجوي إلى تقويض الحقوق الأساسيّة للفلسطينيين/ات في الداخل، الضّفة الغربية وقطاع غزة. مع ذلك، صعدت إسرائيل لمصاف الرّيادة العالميّة في مضمار تكنولوجيا المراقبة مع مطلع القرن الحادي والعشرين، لقد شكّل فجرُ ما تُسميه شوشانا زوبوف بـ رأسمالية المراقبة نظامًا يهدف إلى الرّبح عبر استغلال بيانات مستخدمي التكنولوجيا.[4] مُهِّدَ لرأسمالية المراقبة من خلال شراكاتٍ بين الدّولة والشّركات في الولايات المتحدّة في أعقاب أحداث الحادي عشر من أيلول/سبتمبر 2001. ومع بزوغ الحرب العالميّة على الإرهاب، قايضت الحكومة الأمريكيّة بقوانين محدودة لتنظيم عمل شركات التكنولوجيا النّاميّة لقاء منحها الوصول إلى مناجم بيانات المستخدمين الضّخمة الّتي بحوزة هذه الشّركات—كل ذلك في محاولةٍ لمواكبة ركب قطاع تكنولوجيا المراقبة المدنيّة. يُشير الأستاذ في كلية القانون بجامعة ييل (University Yale) جاك بالكين إلى أنّ موقف الولايات المتّحدة المُعارض للتنظيم قد حوّل الإنترنت والشّركات الخاصّة

---

1 الأمم المتّحدة. غير مؤرّخ. "الإعلان العالمي لحقوق الإنسان." تمّ الولوج للمرج في 5 كانون الأوّل/ديسمبر 2023. https://www.un.org/ar/about-us/universal-declaration-of-human-rights.

2 Sa'di, Ahmad. 2016. Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority. Manchester, UK: Manchester University Press.

3 Zureik, Elia. 2016. Israel's Colonial Project in Palestine: Brutal Pursuit. London: Routledge.

4 Zuboff, Shoshanna. 2019. The Age of Surveillance Capitalism. New York: Hatchett Books. https://www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/?lens=publicaffairs.

التي تستغله لأغراض المراقبة إلى فضاء بلا قانون.[5] تكاثرت الشّركات الخاصّة المُكرّسة لجمع البيانات وتحليلها—وزودت الحكومة بالأدوات والخبرات مقابل إجراءات تنظيمية هزيلة.

كغيرها من الدّول، استفادت إسرائيل من نموذج الولايات المتحدة في المراقبة الحكوميّة وتحقيق الأرباح الشّركاتيّة،[6] حيث عَمِد رؤساء الجهاز الاستخباراتي الإسرائيلي خبراء أمن أمريكيين والرّؤساء التّنفيذيين في قطاع التكنولوجيا لتعظيم نطاق عمل جهاز الاستخبارات الإسرائيلي في الأرض الفلسطينية المحتلة (قطاع غزّة والضّفّة الغربيّة المحتلّة بما فيها القدس الشّرقيّة) لمواكبة المتطلّبات الرّقميّة العصر، ذيّلت هذه المساعي نهاية الانتفاضة الثّانية حيث اعتمدت الآلة العسكريّة الإسرائيليّة المراقبة الشّاملة آليّةً للردع—وسيلةً أرادت بها تجنّب المزيد من العنف بدلًا من تحقيق ذلك بالتّوصّل لحلول سياسيّة دائمة. هكذا نمت وحدّات مثل 8200 (النّسخة الإسرائيليّة من وكالة الأمن القومي الأمريكيّة) من وحدات استخبارات الإشارة السلبية إلى ما وصفه الجنرالات "[ب]ـتجمّع من الشّركات الصغيرة النّاشئة" يضمّ في صفوفه جنودًا يربو عددهم على جُند البحريّة الإسرائيليّة.[7] عكف الجيش على تدريب مجنّداتِه ومجنّديه على القرصنة الهجوميّة، وتطوير التّطبيقات التّكنولوجيّة، وتحليل البيانات. في المقابل، يحرم الجيش الإسرائيلي المدنيين/ات الفلسطينيين/ات الذين يقبعون تحت احتلاله من حقّ حماية الخصوصيّة مقارنة بما يتمتع به الإسرائيليون/ات. لقد اكتسب الجنود الإسرائيليون مِرانًا ودُربة وخبرة في بناء تقنيات المراقبة والأمن المتقدّمة وإدارتها مع قيود ضئيلة على من يمكنّهم مراقبته وأيّ نوعٍ من البيانات يمكنهم جمعه.[8]

أدّى توسّع جهاز المراقبة العسكريّة الإسرائيليّ في الضّفّة الغربيّة إلى تسارع تطوّر اقتصاد التكنولوجيا المتقدّمة في إسرائيل. كما أسهمت العلاقات الوثيقة بين الجيش وقطاع التكنولوجيا الخاص منذ عقود في إرساء قطاع تكنولوجي قوّي يتقدّم صفوف قيادته خبراء من وحدات الاستخبارات العسكريّة الإسرائيليّة. مع ذلك وكما يشير عالم الاجتماع الإسرائيلي نيف غوردون، شهدت صناعات التكنولوجيا المتقدّمة في إسرائيل نموًا غير مسبوق عقب أحداث الحادي عشر من أيلول/سبتمبر في ظلّ تحليق مستويّات الطّلب على التكنولوجيا الأمنيّة والمراقبة عالميًا،[9] بالتّالي انتشرت شركات التكنولوجيا الإسرائيليّة النّاشئة الّتي عكفت تُجرّب وتستكشف مكامن تقنيّات الذّكاء الاصطناعي، وتحليل البيانات، والتجسّس السّيبراني. كذلك، تعزّزت التّحالفات بين إسرائيل والولايات المتحدة الأمريكية، إذ أصبح الجيش الأمريكي، ووكالة الاستخبارات المركزيّة الأمريكيّة، ومكتب التّحقيقات الفيدرالي الأمريكي عملاء دائمين لشركات المراقبة الإسرائيليّة. بحلول عام 2016، أصبحت إسرائيل موطنًا لكبرى شركات المراقبة لكلّ فرد في العالم حتّى اعتُبِرت العاصمة العالميّة الأمن الدّاخلي.[10] في المقابل، وكما أشار الائتلاف الفلسطيني للحقوق الرقمية، أضحت الأرض الفلسطينية المحتلة "ميدانًا لاختبار الأنظمة والتّقنيّات القمعية."[11] لم تنفك فضائح انتهاكات حقوق الإنسان تُلازم صناعة أنظمة المراقبة الإسرائيليّة وتطوّقها في السّنين الأخيرة كما يوضّح التّالي من هذا التّقرير. رغم ذلك، مازالت هذه الصّناعة الإسرائيليّة في ازدهار. فكما تُشير مؤسّسة كارنيغي للسلام الدّولي،ما زالت إسرائيل المصدر الأوّل لبرمجيّات التّجسّس والتّقنيّات الرّقميّة الجنائيّة حتّى صيف 2023.[12] من أصل 74 حكومة تشتري هذه التكنولوجيا من مصادر خاصّة، 54 منها توردّها شركات المراقبة الإسرائيليّة. في تشرين الأوّل/أكتوبر 2023، ذكرت صحيفة هآرتس أن مبيعات الأسلحة والتكنولوجيا السيبرانية الإسرائيليّة قد حلّقت في السنوات القليلة الماضية لمستويات لم تصلها من قبل.[13]

5 Balkin, Jack M. 2017. "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3038939.

6 Goodfriend, Sophia. 2022. "Supply and Demand: The U.S.' Impact on Israel's Surveillance Sector." 7amleh: The Arab Center for the Advancement of Social Media.

7 Goodfriend. 2022. "Point. Click. Occupy." The Baffler, September 12, 2022. https://thebaffler.com/latest/point-click-occupy-goodfriend.

8 Beaumont, Peter. 2014. "Israel's Unit 8200 Refuseniks: 'You Can't Run from Responsibility.'" The Guardian, September 12, 2014, sec. World news .https://www.theguardian.com/world/2014/sep/12/israel-unit-8200-refuseniks-transcript-interview.

9 Gordon, Neve. 2010. "Israel's Emergence as a Homeland Security Capital." In Surveillance and Control in Israel/Palestine. London: Routledge.

10 "The Global Surveillance Industry." 2016. Privacy International. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

11 "The Palestinian Digital Rights Coalition Welcomes the Filing of a Lawsuit against the Israeli Surveillance Tech NSO Group." n.d. Al-Haq. Accessed December 6, 2023. https://www.alhaq.org/advocacy/19810.html.

12 Kot, Steven Feldstein, Brian (Chun Hey). 2023. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. Accessed October 4, 2023. https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

13 Yaron, Oded. October 2 2023. «Record-Breaking Spike in Countries Buying Israeli Arms and Cyber.» Haaretz.https://www.haaretz.com/israel-news/security-aviation/2023-10-02/ty-article/.premium/number-of-countries-israel-sells-arms-and-cyber-to-spikes/0000018a-ea37-d3af-a3ce-ebf75d210000.

ثالثًا. الأرض الفلسطينية المحتلّة مختبرًا للتجارب

منذ أوائل القرن الحادي والعشرين، والسّاسة الإسرائيليون يزعمون أنّ برمجيات التّجسس، وعوامل التّعريف البيومتريّة، والاستطلاع بواسطة الطّائرات دون طيار، والمراقبة بواسطة الكاميرات الّتي طوّرتها شركات التكنولوجيا الخاصّة الإسرائيليّة تعزّز القدرات العسكريّة لإسرائيل، حيث يعمد الجيش غالبًا إلى تعهيد أنشطته البحثيّة والتّطويريّة لهذه الطّائفة من الشّركات.[14] كما يدّعي قادة هذه الصّناعة أنّ الشّركات الخاصّة في إسرائيل يمكن أن تعوّل على علاقتها الوثيقة مع جيش الدّفاع الإسرائيلي للمضي قدمًا في البحث، والتطوير، وتنفيذ التّقنيات الجديدة. كجزء من عملية "التّغذية المزدوجة،" تستقطب وحدات الاستخبارات العسكريّة نخبة موهوبي خريجي المدارس الثانوية للالتحاق بالخدمة العسكريّة، حيث يتلقون تدريبًا وخبرات مهمّة،[15] وبمجرد انتهاء خدمتهم الإلزاميّة، ينضم العديد منهم إلى شركاتٍ ناشئة أو يؤسّسون شركاتهم الخاصّة— غالبًا في مجالات الأمن السّيبراني أو الذّكاء الاصطناعي.

مع توسّع البنية التّحتية للمراقبة الإسرائيليّة في قطاع غزّة والضّفّة الغربيّة بما في ذلك القدس الشّرقيّة خلال العقدين الماضيين، حذّر المناصرون/ات والصّحافيون/ات والأكاديميون/ات الفلسطينيون/ات من أنّ الجيش يستغل الاحتلال لاختبار وتنقيح تقنيّات المراقبة الجديدة الّتي يُتاجر بها في الأسواق العالميّة. وعلى حين يتمتع المدنيون/ات الإسرائيليون/ات بحماية قوية لخصوصيّاتهم بموجب القانون المدني المطبّق عليهم، يحرم جيش الاحتلال المدنيين/ات الفلسطينيين/ات الّذين يعيشون تحت حكمه العسكري من الوصول إلى أيّ سُبلٍ يحمون بها حقوقهم، بالذّات في ظلّ الرّقابة المحدودة جدًا على كيفيّة نشر الجيش تقنيات المراقبة في الأرض الفلسطينية المحتلّة.[16] تعقيبًا على هذه الدّيناميكيّة مؤخّرًا، أشار باحثون/ات ومنظماتٍ حقوقيّة أن الفلسطينيين/ات يشكّلون احتياطيًّا منخفض الثمن للبيانات الأوليّة بالنّسبة لشركات تكنولوجيا المراقبة الخاصة الحريصة على اختبار أنظمتها وتنقيحها قبل تصديرها للخارج.[17]

لطالما أُطّرت الأرض الفلسطينية المحتلة كحقل تجاربٍ للأسلحة الإسرائيليّة ومنتجاتها الأمنيّة، إسرائيل الّتي لم تُغادر قائمة أكبر عشر دول مصدرة للأسلحة طوال العقود الخمسة الماضية.[18] قبل تطوّر قطاع المراقبة الرّقمية والآليّة، عُرِفت إسرائيل بتصديرها رشّاشات الأوزي ودبّابات إلبيت (Elbit) في كافّة أصقاع العالم. في هذا السّياق، يربط الصحفي أنتوني لوينشتاين دور إسرائيل الرّيادي في صناعات السلاح باحتلالها لقطاع غزّة والضفة الغربيّة (بما فيها القدس الشّرقيّة) عام 1967. عن ذلك يكتب لوينشتاين، "طوّرت إسرائيل صناعة أسلحة عالمية المستوى، حيث تختبر مطوّراتِها وتختبرها بسلاسة على الشّعب الفلسطيني الّذي تحتلّه، لتسوّق لأسلحتها بعد ذلك على أنّها مجرّبة على أرض المعركة." ويُضيف أنّ "الشّركات الأمنيّة الإسرائيليّة استفادت كثيرًا من العلامة التّجارية للجيش الإسرائيلي، لتنضم إلى سوق أنجح شركات العالم الأمنيّة."[19] تشير منى شتيّة إلى أنّ صعود صناعة المراقبة العالميّة كان بمثابة هبة ونعمة للصناعات الدّفاعية الإسرائيليّة القويّة الّتي تُغذّيها "تقنيّات المراقبة المستخدمة على الفلسطينيين/ات."[20] ازدادت أعداد الشّركات الخاصة العاملة في مضمار الرّصد الإلكتروني والسّيبراني منذ عام 2001، وذلك مع انضمام حكومات النّاتو إلى ما يسمى بالحرب العالميّة على الإرهاب. في المقابل وكما تبرهن لنا دراسات الحالات أدناه، فإن التّطوير والنّشر غير المقيّد لتقنيات المراقبة آل لتآكل الحقوق الأساسية للفلسطينيين/ات عدا عن تداعياته وظلاله السّلبيّة في الخارج.

رابعًا. حالات دراسيّة

1. برمجيّات التّجسّس

تُعدّ برمجيّات التجسّس نوعًا من البرمجيّات الخبيثة الّتي يُمكن تثبيتها سرًا على الأجهزة الحاسوبيّة؛ إذ تستطيع بأنظمتها المكينة الوصول إلى كلّ ركنٍّ وزاوية في نِظام التّشغيل، من سرقة النّصوص، وتسجيل المكالمات، وتمشيط البريد الإلكتروني وصولًا لتشغيل الكاميرات أو الميكروفونات وتسجيل المحادثات. هذه التّقنيات الّتي كانت يومًا حكرًا على الجيوش المتقدمة تكنولوجيًا، بات بإمكان كل الجيوش وقوّات الشّرطة في العالم شراء هذه التّقنيّات من الشّركات الخاصّة المُنتِجةِ

14 Melman, Yossi. 2022. "A Wild, Dangerous Military-Security Complex Has Seized Power in Israel." Haaretz, January 20, 2022, sec. Israel News. https://www.haaretz.com/israel-news/2022-01-20/ty-article-opinion/a-wild-dangerous-military-security-complex-has-seized-power-in-israel/0000017f-f1b3-df98-a5ff-f3bf79b00000.

15 Mhajne, Anwar. 2023. "Israel's AI Revolution: From Innovation to Occupation." Carnegie Endowment for International Peace. Accessed November 16, 2023. https://carnegieendowment.org/sada/90892.

16 Goodfriend, Sophia. 2022. "How the Occupation Fuels Tel Aviv's Booming AI Sector." Foreign Policy (blog). February 21, 2022. https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/.

17 "الأبارتهايد الرقمي: تكنولوجيات التعرف على الوجه وترسيخ الهيمنة الإسرائيليّة." 2023. https://www.amnesty.org/ar/documents/mde15/6701/2023/ar/

18 Labarge, Blair L. 1988. "The Israeli Defense Industry: Limits to Growth?" The Fletcher Forum 12 (2): 341–58.

19 Lowenstein, Anthony. 2023. The Palestine Laboratory. New York, N.Y: Verso Books, 11

20 Shtaya, Mona. 2021. "Palestine Under Surveillance with Mona Shtaya." Al-Shabaka (blog). Accessed December 6, 2023. https://al-shabaka.org/podcasts/palestine-under-surveillance-with-mona-shtaya/.

لها. وفي مضمار برمجيّات التّجسّس العالميّة، للشّركات الإسرائيليّة مكانتها الوازنة، حيث ساهم قدامى ومخضرمو وحداتها الاستخباراتيّة النخبوية بما لديهم من قِدمة في الخدمة، ومِرانٍ ودربةٍ في القطاع الخاص خلال السّنوات القليلة الماضية. في المقابل، يحذّر منتقدو هذا الواقع من أنّ تفشّي شركات برمجيات التّجسّس الخاصّة يشكّل تهديدًا مُحيقًا بالحقّ في الخصوصيّة على مستوى العالم.

على مرأى ومسمع العالم، كُشف ارتباط الشّركات الخاصّة في مجال السّيبراني بالحكم العسكري الإسرائيلي في الأرض الفلسطينيّة المحتلّة في صيف عام 2021 وخريفه، إذ نُشرت سلسلةٌ من المقالات في كبرى الصّحف تدّعي أنّ برمجيّات التّجسّس الّتي تُصنّعها شركة اِن. اِس. أو. (NSO) الإسرائيليّة لبرمجيّات التّجسّس، قد استهدفت ألوفًا مؤلّفة من المعارضين/ات والعاملين/ات في مجال حقوق الإنسان والسياسيين/ات المعارضين/ات في مُختلِف بقاع العالم.[21] بلغ الغضب ذروته عندما أدرجت وزارة التّجارة الأمريكيّة مجموعة اِن. اِس. أو.، إلى جانب شركات برمجيّات تجسّس أخرى، على قائمتها السّوداء، مانعةً إيّاها من إبرام أي صفقات تجاريّة مع الشّركات الأمريكيّة.[22] ومع أنّ شهرة مجموعة اِن. اِس. أو. كانت مرتكزة على دورها في تصدير التّقانة السّيبرانية الإسرائيليّة إلى الأنظمة الاستبداديّة في شتّى أصقاع الدُّنيا، إلّا أنّه بات جليًا أنّ للشّركة أيضًا دورًا محوريًا ضمن ترسانة المراقبة الإسرائيل المُسلّطة على الأرض الفلسطينية المحتلّة. بالفعل، اكتشف نشطاء حقوقيون استقصائيون في تشرين الثّاني/نوفمبر 2021 برمجيّات تجسّس تابعة لمجموعة اِن. اِس. أو. على هواتف ستّة من المدافعين/ات عن الحقوق المدنيّة للفلسطينيين/ات وثلاثة من كبار مسؤولي السّلطة الفلسطينيّة.[23]

ظهرت هذه المعطيات بُعيد أسابيع قليلة من اتهام الجيش الإسرائيلي لست منظمات حقوق إنسان فلسطينيّة بالإرهاب، حيث كان ثلاثة من المدنيين المُخترقة هواتفهم يعملون في هذه المنظّمات. في هذا السّياق، تؤكّد منظّمة هيومن رايتس ووتش إن الكشف عن برمجيّات التجسس إنما يظهر كيف لمراقبة الجيش الإسرائيلي للفلسطينيين/ات أن "تنتهك حقهم في الخصوصيّة، وتقوّض حريتهم في التعبير وتكوين الجمعيّات، وتهدّد أمنهم الشّخصي وحياتهم." كما أن لتفشي برمجيّات التجسّس التوغليّة "تأثيرًا مروّعًا على المدافعين/ات أو الصّحفيين/ات الّذين قد يمارسون الرّقابة الذّاتية خوفًا من المراقبة المحتملة."[24] نجد صدى ما سبق، بسرديّات الأشخاص الّذين اُخْتُرِقَت هواتفهم، حيث أشار بعضهم ليالٍ بلا نوم، إلى ليالٍ تغص بالقلق النّاجم عن احتماليّة تسجيل هواتفهم لمحادثات الحميمة مع أحبائهم وأطفالهم، لقد ساورهم قلق بأن يُبتر أي شيء يفعلونه أو يقولونه من سياقه ويُستخدم ذريعةً لاعتقالهم.[25] يصف أبي العابودي، المدير التّنفيذي لمركز بيسان للبحوث والتّطوير، ما مرّبه لقناة الجزيرة بأنّه "يتجاوز التنصّت، للترويع، إذ تسيطر برمجيات التجسس سيطرةً كاملةً على الهاتف. يمكنها إجراء المكالمات مع أي شخص، أو إرسال رسائل، كما يُمكنها تنزيل محتوى لم يختره."[26] يتردّد صدى هذه الشّهادات في روايات مدافعين/ات حقوقيّين/ات آخرين من أقطارٍ مختلفة من العالم، جمعهم استهداف تقنيّات شركة اِن. اِس. أو. لخصوصيّتهم.[27]

ليست مجموعة شركة اِن. اِس. أو. الشّركة الإسرائيليّة الوحيدة الّتي طوّرت وما زالت تطوّر وتصدّر هذه التّقنيّات على مستوى العالم. في عام 2021، تمّ العثور على برمجيات خبيثة من صنيع شركة كانديرو (Candiru) الإسرائيليّة على هواتف ساسة، وصحافيين/ات، وباحثين/ات في إيران، واليمن، وإسرائيل، والمملكة المتحدة، وتركيا.[28] أمّا برمجيات التّجسس التي صنعتها شركة سايتروكس (Cytrox) الإسرائيليّة، الّتي تتخذ من أثينا مقرًا لها، فقد تسلّلت لهواتف صحفيين/ات في مصر والاتحاد الأوروبي في عامي 2021 و2022. على ذات الغراف، وجدت برمجيّات تجسّس شركة كوادريم (Quadream)، الّتي باعت أدواتها ومنتجاتها التّقنيّة إلى السّعودية، على هواتف مدافعين/ات حقوقيين/ات وصحفيين/ات في أصقاع وبقاعٍ

21 Washington Post. 2021. "Takeaways from the Pegasus Project," July 18, 2021, sec. Investigations. https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

22 Lyngaas, Sean. 2021. "US Blacklists Israeli Firm NSO Group for Use of Spyware | CNN Business." CNN. November 3, 2021. https://www.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html.

23 Kirchgaessner, Stephanie, and Michael Safi. 2021. "Palestinian Activists' Mobile Phones Hacked Using NSO Spyware, Says Report." The Guardian, November 8, 2021, sec. World news. https://www.theguardian.com/world/2021/nov/08/palestinian-activists-mobile-phones-hacked-by-nso-says-report.

24 " استخدام برنامج تجسس لاختراق المدافعين الحقوقيين الفلسطينيين." هيومن رايتس ووتش، 2021، (مدوّنة). 8 تشرين الثّاني/نوفمبر، 2021. https://www.hrw.org/ar/news/2021/11/08/380353

25 Bajak, Frank, and Joseph Krauss. 2021. "Report: NSO Spyware Found on 6 Palestinian Activists' Phones." AP News. November 8, 2021. https://apnews.com/article/technology-business-israel-jamal-khashoggi-hacking-6bfc5bc992de7f33f5c8e969e69ce15c.

26 Staff, Al Jazeera. 14 Nov. 2021. "Palestinian Rights Activists Defiant over Israeli Spyware Hacks." Al Jazeera. Accessed December 6, 2023. https://www.aljazeera.com/news/2021/11/14/palestinian-rights-activists-defiant-over-israeli-spyware-hacks.

27 Carey, Matthew. 2021. "'Terror Contagion' Director Laura Poitras On Dangers Of Israeli Company's Pegasus Malware: 'It's Classified As A Cyber Weapon.'" Deadline (blog). December 11, 2021. https://deadline.com/2021/12/terror-contagion-neon-short-documentary-director-laura-poitras-interview-news-1234889177/.

28 Megiddo, Gur. 2021. "'We're on the U.S. Blacklist Because of You': The Dirty Clash between Israeli Cyberarms Makers." Haaretz, December 17, 2021, sec. Israel News. https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000.

مختلفة من العالم في عام 2023.[29]

لا يمكن التّقليل من صِلة علاقات هذه الشّركات والجيش الإسرائيلي بأي شكلٍ من الأشكال. في عام 2018، ذكرت صحيفة هآرتس أن 80 في المئة من مؤسّسي 700 شركة سيبرانية في إسرائيل والبالغ عددهم 2300 شخص هم من قدامى كوادر وحدات الاستخبارات العسكريّة الإسرائيليّة. [30] بعد عامين من هآرتس، وجدت صحيفة نيويورك تايمز أنّ كل عضو تقريبًا في فريق بحوث مجموعة اِن. اِس. أو. كان قد عمِلَ في مُديريّة المخابرات العسكريّة الإسرائيليّة. كذلك، فإن مؤسّسي شركات التّجسس الإسرائيليّة الكبرى مثل كانديرو، سايتروكس، وإنتلكسا (Intellexa) سبق وأن تبوؤوا مناصب قياديّة في الاستخبارات العسكريّة الإسرائيليّة، بل كان بعضهم مسؤولًا عن تطوير ونشر الأسلحة السّيبرانية في الأرض الفلسطينيّة المحتلّة.[31]

تتجاوز علاقات هذه الشّركات بالجيش الإسرائيلي الأطر المهنية، إذ لم ينفك الجيش يُعهّد جزءًا كبيرًا من الأنشطة التّطويريّة التقنيّة المرتبطة بالأمن السّيبراني لهذه الشّركات الخاصّة، ما يوفّر لشركات المراقبة النّاشئة فرصةً فريدة لصقل منتجاتها قبل تصديرها للعالم، وذلك عبر تجربتها على المدنيين/ات الفلسطينيين/ات الذين يرزحون تحت الحكم العسكري الإسرائيلي. تلك العلاقة المتبادلة، الّتي لا يمكن الاستهانة بها أو غضّ الطّرف عنها، قد مهدت الطّريق للتساهل في الضّوابط النّاظمة للأنشطة التّصديريّة لشركات مثل مجموعة اِن. اِس. أو.، الّتي تتجاوز منتجاتها حدود السّلعة لتكون أوراقًا دبلوماسيّة في الحبكات الجيوسيّاسة الإقليميّة. يُذكر في هذا السّياق أن المكاسب الدّبلوماسية الإسرائيليّة (كإقامة علاقات رسميّة مع دول المنطقة وغيرها) غالبًا ما سبقتها صفقات لبيع منتجات مجموعة اِن. اِس. أو.[32]

تضرّرت سمعة مجموعة اِن. اِس. أو. إلى حدٍّ بعيد عقب الكشف عن ممارساتها عام 2021، وذلك بفضل تضافر جهود صحفيين/ات استقصائيين/ات من مختلف أرجاء المعمورة. في المقابل، تعهدّت إسرائيل بتبني قوانين تصدير أكثر صرامة، محددةً بذلك المنتجات الّتي يمكن للشركات الإسرائيليّة بيعها للحكومات الأجنبيّة. في نيسان/أبريل 2023، أفادت صحيفة كالكاليست (Calcalist) بأنّ صناعة برمجيات التّجسس الإسرائيليّة قد تقلصت بوضوح في السّنين الأخيرة، حيث نقلت العديد من الشرّكات الإسرائيليّة مقرّاتها إلى الخارج، أو غيرت تركيز نشاطها في حال بقائها في إسرائيل. [33] ومع ذلك، استمرت الحكومة الإسرائيليّة في الحفاظ على علاقات وثيقة مع شركات مثل مجموعة اِن. اِس. أو. وكانديرو، حيث جنحت الخدمات الأمنيّة الإسرائيليّة لاستخدام منتجات الشركتين المذكورتين عقب اندلاع الحرب مع قطاع غزّة في السّابع من تشرين الأوّل/أكتوبر في خطوة شكّلت تراجعًا حادًا عن السّياسات السّابقة. [34]ومنذ ذلك الحين، قامت مجموعة اِن. اِس. أو. وكانديرو بتقديم خدماتهما تطوّعًا لدعم الجهد الحربيّ الإسرائيلي، حيث قدّمتا أنظمتهما لتحديد مواقع الرّهائن الإسرائيليين داخل غزّة، ممّا يشير إلى أن العلاقات طويلة الأمد بين المسؤولين الإسرائيليين وهذه الشّركات المنبوذة لم تنقطع يومًا. ووفقًا لوثائق حصل عليها موقع الإنترسبت، فقد عرضت مجموعة اِن. اِس. أو. خدماتها على الحكومة الأمريكية أيضًا. [35] في ضوء ذلك، يبقى سؤال كيفيّة استجابة هذه الصّناعة للحرب المشتعلة في المنطقة أمرًا لا بّد من رصده ومراقبته، مع ذلك ثمَّ مُعطى واضح في هذه المسألة، ألا وهو أنّ استخدام إسرائيل لهذه التّقنيّات ضد الفلسطينيين/ات أسفر إلى تفشّي نظمٍ تسبّبت بتآكل حقّ الخصوصيّة في معظم السياقات الّتي وُظّفَت فيه هذه التّقنيّات.

2. مراقبة منصّات التّواصل الاجتماعي

برزت وسائل التّواصل الاجتماعي كأداةٍ رئيسة في الآلة الإسرائيليّة لمراقبة للأراضي الفلسطينيّة المحتلّة فور انتشار استخدامها في المنطقة في أواخر العقد الأوّل من القرن الحادي والعشرين. إذ أدّت هذه المنصّات دورًا جوهريًا في حركات الاحتجاج الّتي عمّت أرجاء الشّرق الأوسط خلال ما عُرِف بالربيع العربي—بما في ذلك الأرض الفلسطينية المحتلة، حيث شكّلت منصات كفيسبوك وإنستغرام وتيك-توك نقطة تجمّع لهذه الحِراكات. استشعارًا لذلك طفق جهاز المخابرات العسكريّة الإسرائيليّة يطوّر أساليب مراقبةٍ أكثر تطفلًا ودقّة للفضاءات الرّقميّة الفلسطينيّة—من الخوارزميات البوليسيّة التنبؤية وروبوتات

29 Kabir, Omer. 2023. “Is Israeli Spyware a Dying Sector?” Ctech. April 20, 2023. https://www.calcalistech.com/ctechnews/article/twcgg3tql.

30 Shezaf, Hagar, and Jonathon Jacobson. 2018. “Revealed: Israel’s Cyber-Spy Industry Helps World Dictators Hunt Dissidents and Gays - Israel News - Haaretz.Com.” Haaretz, October 20, 2018. https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.

31 Kot, Steven Feldstein, Brian (Chun Hey). n.d. “Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.” Carnegie Endowment for International Peace. Accessed November 16, 2023. https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

32 Bergman, Ronen, and Mark Mazzetti. 2022. “The Battle for the World’s Most Powerful Cyberweapon.” The New York Times, January 28, 2022, sec.Magazine.https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

33 Kabir, Omer. 2023. “Is Israeli Spyware a Dying Sector?” Ctech. April 20, 2023. https://www.calcalistech.com/ctechnews/article/twcgg3tql.

34 Newman, Marissa. 2023. “Israel Taps Blacklisted Pegasus Maker to Track Hostages in Gaza.” Bloomberg.Com, October 26, 2023. https://www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas.

35 Gee, Georgia. 2023. “Israeli Spyware Firm NSO Demands ‘Urgent’ Meeting With Blinken Amid Gaza War Lobbying Effort.” The Intercept. November 10, 2023. https://theintercept.com/2023/11/10/nso-group-israel-gaza-blacklist/.

جمع البيانات من وسائل التّواصل الاجتماعي لتحديد وسوم المحتوى الذي يُزعم باحتوائه على طابع تحريضي.[36] يُشير الصحفيون/ات إلى أنّ هذه التّرسانة المتطورة من أدوات المراقبة تعمل بالتّوازي مع ترسانة أخرى منَ قوانين التحريض التّمييزية التي تجرّم العديد من أشكال الخطاب السّياسي الفلسطيني.[37] ففي عام 2016، عَمِد الكنيست الإسرائيلي إلى توسيع نطاق التّعريف القانوني للتحريض لكي لا يقتصر على الخطاب الّذي "يدعو مباشرة إلى العنف" بل ليشمل أي خطاب يُعتبر، في نظر الادعاء الإسرائيلي العام "داعمًا للأعمال الإرهابية،" سواء أكان هناك نيّة لتنفيذها أم عُدِمت تلك النّية.[38]

اعتمدت إسرائيل في مراقبتها العسكريّة على وسائل التّواصل الاجتماعي على أساليب سلبية وأخرى فاعلة لرصد الفضاءات الرّقمية الفلسطينيّة. في سلّة وسائلها السّلبيّة، نجد أدوات لجمع البيانات من وسائل التّواصل الاجتماعي لفحص المحتوى الفلسطيني، معتمدةً بشكل متزايد على الذّكاء الاصطناعي في تحليل البيانات، وتحديد المحتوى الإجرامي، والتّنبؤ بالمستخدمين/ات الّذين يُرجّح لارتكابهم أعمال مخالفة للقوانين والأنظمة الإسرائيلية. تشير التّقارير الحديثة إلى انحدار وتدنيّ دقّة الخوارزميات البوليسيّة التنبؤية.[39] أمّا على صعيد المراقبة الفاعلة، تستخدم إسرائيل الذّكاء الاصطناعي التّوليدي لإنشاء حساباتٍ وهمية تنشر معلومات ودعايات مضللة كما برامج قادرة على اختراق الحسابات الخاصة. في عام 2018، ذكرت صحيفة هآرتس أنّ هذه الجهود وُحِّدَت تحت مسمى "مركز عمليات الوعي،" وهي وحدة مكرّسة لشن عمليات نفسيّة سرّيّة عبر الإنترنت، يشمل نطاق عمل هذا المركز الأرض المحتلّة والعالم أجمع.[40] في أعقاب حرب عام 2021 بين إسرائيل وحماس الّتي اشتعلت جرّاء الاحتجاجات التاريخية في القدس الشّرقيّة المحتلّة، والمعروفة أيضًا باسم انتفاضة الوحدة أو هبّة الشّيخ جراح، زعمت هآرتس أنّ أجهزة الأمن الإسرائيليّة اعتمدت على حسابات وهميّة لنشر أخبار كاذبة عبر وسائل التّواصل الاجتماعي وتطبيقات المراسلة المشفّرة، بما في ذلك تيليجرام.[41] كما تستخدم القوّات العسكريّة وأجهزة الأمن الإسرائيليّة الذّكاء الاصطناعي لمراقبة ووسم المحتوى الفلسطيني على وسائل التّواصل الاجتماعي. في سياق متصل عام 2023، صرّح رئيس أجهزة الأمن الإسرائيليّة أنّ الذكاء الاصطناعي كان "مُساعدًا" في تنفيذ العمليّات التي يقوم بها جيش الدّفاع الإسرائيلي.[42]

تزامن توظيف تقنيّات المراقبة المتقدّمة في رصد وسائل التّواصل الاجتماعي مع صدور تقارير تشير إلى تزايد القمع الإسرائيلي للفلسطينيين/ات وتآكل حقوق الأساسية مثل حرّيّة التّعبير والحق في التجمّع وتكوين جمعيات. تذكر مجلة 972 في هذا السّياق أنّ عمليّات الاعتقال والتّوقيف بسبب منشوراتٍ على وسائل التّواصل الاجتماعي قد ارتفعت في السّنوات الأخيرة، خاصّة في صفوف الفلسطينيين/ات المقدسيين/ات.[43] يشير تقرير أصدرته حملة عام 2021 إلى أنّ العديد من الشّباب الفلسطيني يشعر بأن استشراء المراقبة على الإنترنت وخارجها يشكل نوعًا آخر من الحبس.[44] كذلك تؤكّد التّقارير الأخيرة لتعاظم المراقبة الإسرائيليّة للنشاط الفلسطيني على وسائل التواصل الاجتماعي منذ بداية الحرب الإسرائيليّة على غزة.[45] في تشرين الثّاني/نوفمبر، قدم الكنيست الإسرائيلي تعديلًا على قانون مكافحة الإرهاب يجرّم "استخدام وسائل الإعلام الإرهابية." وقد تُرجم ذلك بتعريض فلسطيني/ات الضّفّة الغربيّة وإسرائيل والقدس لمراقبةٍ مكثّفة بالتّزامن مع ما استُحدِث من تشريعات تغالي أكثر في تجريم الأنشطة الفلسطينيّة على الإنترنت. يقول الخبراء القانونيون إن هذا النّوع من المراقبة الشّاملة يؤثر سلبًا على الفلسطينيين/ات في كل أنحاء المنطقة.[46] ووفقًا لمركز عدالة فإنّ هذه الإجراءات مجتمعةً

---

36 Fatafta, Marwa, and Nadim Nashif. 2017. "Surveillance of Palestinians and the Fight for Digital Rights." Al-Shabaka (blog). Accessed December 6, 2023. https://al-shabaka.org/briefs/surveillance-palestinians-fight-digital-rights/.

37 Goodfriend, Sophia. 2021. "When Palestinian Political Speech Is 'Incitement.'" Jewish Currents. September 15, 2021. https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.

38 "Israel's New Counter-Terrorism Law and Terrorism in Cyberspace." n.d. Council on Foreign Relations. Accessed November 16, 2023. https://www.cfr.org/blog/israels-new-counter-terrorism-law-and-terrorism-cyberspace.

39 "Study Finds Predictive Policing Software Is Actually Pretty Terrible at Predicting Crimes." 2023. Gizmodo. October 3, 2023. https://gizmodo.com/predictive-policing-cops-law-enforcement-predpol-1850893951.

40 Harel, Amos. 2018. "Israeli Army Sets Up 'Consciousness Ops' Unit to Influence Enemy Armies, Foreign Media and Public Opinion." Haaretz. March 10, 2018. https://www.haaretz.com/israel-news/2018-03-10/ty-article/with-eye-on-hearts-and-minds-israeli-army-sets-up-consciousness-ops/0000017f-eff4-d223-a97f-effdab210000.

41 "Study Finds Predictive Policing Software Is Actually Pretty Terrible at Predicting Crimes." 2023. Gizmodo. October 3, 2023. https://gizmodo.com/predictive-policing-cops-law-enforcement-predpol-1850893951.

42 Reuters. 2023. "Israel's Shin Bet Spy Service Uses Generative AI to Thwart Threats | Reuters," June 27, 2023. https://www.reuters.com/technology/israels-shin-bet-spy-service-uses-generative-ai-thwart-threats-2023-06-27/.

43 Reiff, Ben. 2023. "For Palestinians, Social Media Influence Comes with the Threat of Prison." +972 Magazine. October 2, 2023. https://www.972mag.com/palestinian-influencers-social-media-persecution/.

44 Goodfriend, Sophia, Bashar Bakri, and Rawan Sheikh Ahmad. 2021 "Intensification of Surveillance in East Jerusalem and Impact on Palestinian Residents' Rights: Summer and Fall 2021." Accessed November 17, 2023. https://7amleh.org/2021/11/08/intensification-of-surveillance-in-east-jerusalem-and-impact-on-palestinian-residents-rights-summer-and-fall-2021.

45 Kermanitzer, Mordechai. 2023. *"החוק האוסר צריכה של פרסומי טרור עלול לשמש לרדיפת אזרחים ערבים - מדיני ביטחוני - הארץ."* Haaretz. October 25, 2023. https://www.haaretz.co.il/news/politics/2023-10-25/ty-article/0000018b-676d-d326-a39b-677d1e110000.

46 "Israeli Knesset Passes Draconian Amendment to the Counter-Terrorism Law Criminalizing - Adalah." n.d. Accessed November 17, 2023. https://www.adalah.org/en/content/view/10951.

تجسّد "حملة قمع ضارية على حقوق الفلسطينيين/ات وحرّيتهم في التّعبير، عدا ما تنثني عليه من اضطهادٍ سياسيٍّ للفلسطينيين كجماعة."[47]

شهدت السّنوات الأخيرة بيع شركات المراقبة الإسرائيليّة تقنيات مماثلة في السّوق الخاصّة، واتهم بعض هذه الشّركات بسرقة بيانات مستخدمي وسائل التّواصل الاجتماعي بطرق مخالفة للقانون ولأهدافٍ ربحيّة. في عام 2018، رفعت شركة ميتا دعوى قضائية على الشّركة الإسرائيليّة فوياجر لابس (Labs Voyageur) بتهمة استخدام نحو أربعين ألف حسابٍ وهميٍّ على فيسبوك لجمع بيانات زهاء 600000 مستخدم. [48]في سياق مماثل عام 2020، حرّكت ميتا دعوى قضائيّة أخرى بحق الشركة الإسرائيليّة براند توتال (BrandTotal) بتهمة الاستخلاص غير القانوني للبيانات الشّخصيّة من حسابات المستخدمين/ات، بما في ذلك أسماؤهم، وهويّاتهم، وجنسهم، وتواريخ ميلادهم، وحالتهم العاطفية، ومعلومات الموقع خاصّتِهم. [49] أيضًا شهد عام 2023 رفع ميتا واِكس (المعروفة سابقًا باسم تويتر) دعوى قضائيّة على الشركة الإسرائيليّة برايت داتا (Data Bright) بتهمة استخلاص محتوى المستخدمين/ات من فيسبوك، انستغرام، وتويتر وبيعه. [50] في أيلول/سبتمبر من ذات العام، كشف تحقيق أجرته هآرتس أن الشّركات الإسرائيليّة كانت تبيع أيضًا نسخًا أكثر تطفلًا من هذه التقنيات كخدمات مراقبة لدولٍ أجنبية، [51] حيث خَلُص التحقيق أن شركتي إنسانِت (Insanet) ورايزون (Rayzone) قد طوّرتا أنظمة لا تقتصر فقط على استخلاص حسابات المستخدمين/ات على وسائل التّواصل الاجتماعي، بل تتجاوز ذلك للتسلّل إلى هواتفهم من خلال تجاوز حمايات الأمان الرّاهنة وصولًا لسرقة بياناتهم الحسّاسة. وفقًا لهآرتس، تأسست هاتان الشركتين على أيدي "أعضاء سابقين في هيئة الدفاع الإسرائيليّة" "[و]رجال أعمال متسلسلين" في قطاع الصّناعات السيبرنيّة الإسرائيليّة.

أحد هذه الشرّكات، وهي شركة فريق خورخي (Jorge Team) الإسرائيليّة للمرتزقة السيبرانية، كانت متورطة في واحدة من أخطر فضائح حقوق الإنسان في السنوات الأخيرة، إذ كُشف تعاون شركة كامبريدج أناليتيكا (Analytica Cambridge)، الشرّكة الاستشاريّة البريطانية الّتي سرقت بيانات ملايين من مستخدمي/ات فيسبوك للتأثير في نتائج الانتخابات الدّيمقراطية في عدّة بقاعٍ من العالم مع شركة فريق خورخي التي تتألف من قدامى كوادر وحدات الاستخبارات الإسرائيليّة. بينما أوقفت كامبرِيدج أناليتيكا عن العمل بعد رفع دعوى قضائية عليها من لجنة التّجارة الفيدرالية الأمريكيّة بسبب استخلاصها للبيانات بطرائق غير قانونيّة، تواصل شركة فريق خورخي أعمالها بسريّة. في عام 2023، كشف تحقيق لمنظّمة فوربيدن ستوريز (Stories Forbidden) أنّ شركة فريق خورخي تدخّلت في الانتخابات الدّيمقراطية في إفريقيا لسنوات، حيث باعت الشركة برمجيات لنشر المعلومات المضللة وأدوات قرصنة اخترقت البُرد الإلكترونيّة للأطراف المُستهدفة كما حساباتهم على تطبيقات المراسلة لتحقيق أغراض سياسية، وذلك في كينيا ونيجيريا في أواخر العقد الأول وأوائل العقد الثّاني من القرن الحادي والعشرين. [52] وفقًا لصحيفة الغارديان، فقد تفاخر مؤسّس فريق خورخي تال حنان، بنشر معلومات مضللة خلال انتخابات عام 2019 في السّنغال. وزعم حنان أنه تدخل في 33 انتخابات رئاسية في أقطار القارة الإفريقية. [53] وثق الصحفيون/ات بدورهم كيف أسفر هذا التّدخل عن انتهاك حرّية التّعبير والحق في الخصوصيّة في كل سياق تم فيه توظيف هذه التّكنولوجيا التوغليّة.[54]

تشهد سوق تقنيات المراقبة الاجتماعيّة التوغلية ازدهارًا رهيبًا، وتعدّ الشّركات الإسرائيليّة من اللّاعبين الرئيسين في هذه الصّناعة غير المنظّمة إلى حدٍ بعيد. وفي خضم كل ذلك، يوضّح الأثر المروّع للمراقبة الشّاملة والمعلومات المضلّلة على مستخدمي/ات وسائل التواصل الاجتماعي الفلسطينيين/ات المخاطر الّتي تجسّدها هذه التقنيات على مستوى العالم أجمع.

---

47 "Crackdown on Freedom of Speech of Palestinian Citizens of Israel." 23 Oct. 2023 Adalah: The Legal Center for Arab Minority Rights in Israel. Accessed December 6, 2023. https://www.adalah.org/en/content/view/10925.

48 Bhuiyan, Johana. 2023. "NYPD Spent Millions to Contract with Firm Banned by Meta for Fake Profiles." The Guardian, September 8, 2023, sec. USnews.https://www.theguardian.com/us-news/2023/sep/08/new-york-police-tracking-voyager-labs-meta-contract.

49 Whittaker, Zack. 2020. "Facebook Sues Two Companies Engaged in Data Scraping Operations." TechCrunch (blog). October 1, 2020. https://techcrunch.com/2020/10/01/facebook-sues-two-companies-engaged-in-data-scraping-operations/.

50 Wrobel, Sharon. 2023. "Musk's X Corp Sues Israel's Bright Data for Scraping Data." Times of Israel. July 27, 2023. https://www.timesofisrael.com/musks-x-corp-sues-israels-bright-data-for-illegally-scraping-data/.

51 Benjakob, Omer. 2023. "Revealed: Israeli Cyber Firms Have Developed an 'insane' New Spyware Tool. No Defense Exists." Haaretz, September 14, 2023, sec. Israel News. https://www.haaretz.com/israel-news/2023-09-14/ty-article-magazine/.highlight/revealed-israeli-cyber-firms-developed-an-insane-new-spyware-tool-no-defense-exists/0000018a-93cb-de77-a98f-ffdf2fb60000.

52 Gur Meggido and Omer Benjakob. 2023. "The Israeli Hackers Who Tried to Steal Kenya's Election." Haaretz, February 15, 2023. https://www.haaretz.com/israel-news/security-aviation/2023-02-15/ty-article-magazine/.premium/the-israeli-hackers-who-tried-to-steal-kenyas-election/00000186-4b7f-d5d4-a5e7-ebff5c9c0000.

53 Kirchgaessner, Stephanie, and Jason Burke. 2023. "Political Aides Hacked by 'Team Jorge' in Run-up to Kenyan Election." The Guardian, February 15, 2023, sec. World news. https://www.theguardian.com/world/2023/feb/15/political-aides-hacked-by-team-jorge-in-run-up-to-kenyan-election.

54 "In Nigeria, 'Team Jorge' Hackers Collaborated with Cambridge Analytica," Le Monde. February 17, 2023. https://www.lemonde.fr/en/pixels/article/2023/02/17/in-nigeria-team-jorge-hackers-collaborated-with-cambridge-analytica_6016268_13.html.

3. تقنيّات التّعرّف على الوجوه

شهد نطاق استخدام كاميرات التّعرف على الوجوه توسّعًا في الضّفّة الغربيّة والقدس الشّرقيّة في الآونة الأخيرة، وقد تحقّق ذلك عبر التّعاون الوثيق بين الشّركات الخاصّة المتخصّصة في تقنيّات التّعرف على الوجوه والجيش الإسرائيلي. لكن استخدام الجيش الإسرائيلي للمراقبة البيومترية ليس بالأمر الجديد. فقد ألزم الجيش الإسرائيلي الفلسطينيين/ات باستخدام بطاقات تعريف بيومترية إن أرادوا استصدار تصاريح للعمل أو الدّراسة داخل إسرائيل، وذلك منذ أوائل العقد الأوّل من الألفيّة الجديدة، ممّا يتطلب منهم تقديم بياناتهم البيومترية للجيش الإسرائيلي. [55] في ذات السّياق، توّسع استخدام الجيش للمراقبة البيومترية كثيرًا مع التّقدم تقنيّات معالجة الصّور والمراقبة العاملة بالخوارزميّات. وحسب لتقاريرٍ صادرة عن مركز أبحاث «مَن يستفيد» (WhoProfits) فقد قامت الشّرطة الإسرائيليّة بتحديث شبكة كاميرات المراقبة التلفزيونية المغلقة الّتي تغطي مدينة القدس القديمة بتقنيّات التعرف على الوجوه عام 2017، [56] وبحلول أواخر العقد الأول من القرن الحالي، قامت السّلطات الإسرائيليّة بتركيب كاميرات التّعرف على الوجوه في الحواجز العسكريّة الرئيسة التي تؤدي إلى الضّفّة الغربيّة المحتلّة.

في عام 2019، سلطت تقارير استقصائية الضّوء على القضايا الأخلاقية المتعلقة بالمراقبة البيومترية للفلسطينيين/ات. في هذا العام أيضًا كشفت شبكة إن. بي. سي. (NBC) عن تركيب كاميرات جديدة للتعرف على الوجوه في القدس الشّرقيّة ووضعها في أماكن مخفيّة في أرجاء الضّفّة الغربيّة. وشهدت السّنوات الّتي تلت ذلك، تزايدًا في استخدام السّلطات الإسرائيليّة لهذه التكنولوجيا. في عام 2021، كشفت تقارير استقصائيّة لصحيفة واشنطن بوست عن قيام الجيش الإسرائيلي ببناء قاعدة بيانات بيومترية تُعرف بـ "نِظام الذّئب الأحمر للتعرّف على الوجوه،" تضم بيانات جميع المدنيين/ات الفلسطينيين/ات في الضّفّة الغربيّة دون موافقتهم. [57] ارتبطت هذه القاعدة بتطبيقٍ حمل نفس اسمها وثُبّت على الأجهزة اللوحية التي يحملها الجنود الإسرائيليّون في الضّفة الغربيّة. من الجدير بالذّكر أنّ تكوين هذه الأنظمة قائم على ممارسات توغلية تُفتّت خصوصية المدنيين/ات، شمِل ذلك على سبيل المثال لا الحصر، إيقاظ أطفالٍ من نومهم لمسح وجوههم وتسجيلهم في قاعدة الذّئب الأحمر البيومتريّة، أو إيقاف تلاميذ في طريقهم إلى المدرسة لتغذيّةً قاعدة الذّئب الأحمر. [58] وفي عام 2023، زعمت منظمتا العفو الدّولية وكسر الصّمت أن المراقبة البيومترية قد توسعت لتشمل الحواجز العسكريّة الصّغرى في الضّفّة الغربيّة، لا سيّما الخليل. [59]

من الجدير بالذكر أيضًا أنّ الشّركات الإسرائيلية الخاصّة ضالعة بتعاونها مع الجيش لبناء هذه الأنظمة وتنقيحها. يصف المحامي عيسى عمرو المدن الفلسطينيّة التي تغيّرت بفعل هذه الأنظمة الجديدة بأنّها أضحت "مختبرَ تجاربٍ لشركات الحلول الأمنيّة [الإسرائيليّة] لاختبار تقنيّاتها وتسويقها أيضًا." [60] تم تطوير وتركيب نظام المراقبة مبات 2000 (Mabat 2000) في القدس الشّرقيّة بواسطة مجموعة مير (Mer)، وهي شركة أمن إسرائيليّة تعاقد معها جيش الدّفاع الإسرائيلي مرارًا. [61] أفادت صحيفة ذا ماركِر (Marker The) بأنّ شركة تقنيّات التّعرف على الوجه الإسرائيليّة أوستو (Oosto) المعروفة سابقًا باسم آني-فِجين (AnyVision) قد صنّعت كاميرات بيومترية في الحواجز العسكريّة الرئيسة وقدّمة خدماتها في هذا الصّدد أيضًا. [62] زعمت شبكة إن. بي. سي. أن الشّركة ذاتها ركبت كاميراتها في القدس الشّرقيّة، [63] لكن بحسب صحيفة الغارديان، فإنّ الشركتين الصّينيتين هِك-فِجن (Hikvision) تي. كاي. اِتش. سِكيورِتي (Security TKH) هما من تصنّعان الكاميرات البيومترية المستخدمة في القدس والخليل. [64] وقد تم ربط شركة هِك-فِجن أيضًا بالمراقبة والاحتجاز الجماعي للأويغور

---

55 Spektor, Michelle. 2020. "Imagining the Biometric Future: Debates Over National Biometric Identification in Israel." Science as Culture; Abingdon 29 (1). https://www-tandfonline-com.proxy.lib.duke.edu/doi/abs/10.1080/09505431.2019.1667969.

56 "Big Brother in Jerusalem's Old City." 2018. Who Profits. https://www.whoprofits.org/writable/uploads/old/uploads/2018/11/surveil-final.pdf

57 Dwoskin, Elizabeth. 2021. "Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank." Washington Post, November 8, 2021. https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

58 Goodfriend, Automated State Violence

59 Shezaf, Hagar. 2023. "Israel Using Facial Recognition Technology to Entrench Apartheid, Amnesty International Says." https://www.haaretz.com/israel-news/2023-05-02/ty-article/.highlight/israel-using-facial-recognition-tech-to-entrench-apartheid-amnesty-intl-says/00000187-db8a-d9b4-abaf-fbbe6c080000?lts=1699971580597.

60 Siddiqui, Usaid. 2023. "'Chilling Effect': Israel's Ongoing Surveillance of Palestinians." Al Jazeera. May 7, 2023. https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians.

61 Who Profits, "Mabat 2000"

62 Ziv, Amitai. 2019. "Anivision: The Intriguing Israeli Start-up That Operates Secretly in the Territories." The Marker, July 14, 2019. https://www.themarker.com/technation/2019-07-14/ty-article/.premium/0000017f-e19e-df7c-a5ff-e3fe311d0000.

63 Solon. 2019. "Microsoft Funded Firm Doing Secret Israeli Surveillance on West Bank." NBC News, October 28, 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116.

64 Bhuiyan, Johana. 2023. "How Chinese Firm Linked to Repression of Uyghurs Aids Israeli Surveillance in West Bank." The Guardian, November 11, 2023, sec. Technology. https://www.theguardian.com/technology/2023/nov/11/west-bank-palestinians-surveillance-cameras-hikvision.

شمالي غرب الصين، عدا أنّها مدرجة على القائمة السّوداء لوزارة التّجارة الأمريكيّة.[65]

يُعدّ تطبيق الجيش الإسرائيلي للمراقبة البيومترية جزءًا من تحرّك رسمي نحو احتلال "خالٍ من الاحتكاك،" فقد وعد مسؤولون بجيش الدّفاع أنّ التّقنيات الجديدة ستُقلل التّفاعلات المُهينة بين الجنود والفلسطينيين/ات، مثل التفتيش الجسدي واقتحام المنازل، وذلك بترك مهمة التّعريف للآلات بدلًا من الجنود،[66] لكن هذه الوعود لاقت ما يناقضها في تقارير منظّمات حقوق الإنسان الكبرى والباحثين/ات والصحفيين/ات. وجدت مجلة فورين بوليسي (Policy Foreign) أنّ تطبيق المراقبة الآليّة زاد تدخّل الجيش في حياة الفلسطينيين اليوميّة.[67] ففي الخليل، على سبيل المثال، نصب الجيش كاميرات جديدة على أسطح منازل الفلسطينيين، ولصيانة هذه التكنولوجيا، لم يتوان الجنود عن دخول البيوت الّتي نُصّبت عليها الكاميرات في ممارسة تُمعن في تآكل الخصوصية. وفي القدس، وصف باحثو/ات من منظّمة العفو الدّوليّة كيف تسبّبت تفشّي الكاميرات بحالة قلقٍ العديد من النّساء اللّواتي بتن يخشين بأن الجيش يراقبهن حتى في حُرمة منازلهن.[68] تُعاضد هذه النتائج تقريرًا كانت أصدرته حملة عام 2021، يصف هذا التّقرير كيف تسبب انتشار الكاميرات في القدس بدفع ساكني المدينة الفلسطينيين للشعور بأنّهم مراقبون حتى وهم في منازلهم حتّى أضحوا هم يراقبون أنفسهم، يُترجم ذلك ببقائهم بملابس الخروج في البيت أو إبقاء النّساء غطاء رأسهن حتّى وهنّ في عقر دارهن.[69]تصف عالمة الاجتماع نادرة شلهوب - كيفوركيان هذه المراقبة بأنّها "صناعة رعب" تولّد الخوف في نفوس أولئك الذين يخضعون لآليات المراقبة التوغّلية، لا سيّما النّساء.[70]

تُشير آثار هذه الأنظمة في الأرض الفلسطينية المحتلة إلى أن المراقبة البيومترية، التي تُنفّذ باسم تقليل العنف، تُفاقم شعور الفلسطينيين/ات بالعوز الأمان في ظلّ ما يتعرّضون له من رصدٍ وعسكرة مكثّفة تزيد تآكل حقّهم الأساسي في الخصوصّية. تتعارض هذه النّتائج مع ادعاءات شركات التّقنيّات البيومتريّة النّاشئة الّتي تعد بأنّ الاستخدام غير المقيّد لهذه التكنولوجيا سيعزز الأمن ويقلّل العنف. على الرغم من الفعالية المشكوك فيها لهذه الأنظمة، ثمّ تعاظم في ميل الحكومات وجهات إنفاذ القانون إلى تبني المراقبة البيومترية، الأمر الّذي ترى فيه الشركات الإسرائيليّة طلبًا تسعى لتلبيته.[71]

خامسًا. تحليل قانوني والتّداعيات الحقوقيّة

بموجب القانون الدولي، يُعدّ الجيش الإسرائيلي قوّة قائمة بالاحتلال وبتّالي مسؤول عن حماية "الحياة المدنية" للفلسطينيين/ات في قطاع غزّة، والضّفّة الغربيّة بما فيها القدس الشّرقيّة،[72]بيد أنّ البحوث والتقارير الملخّصة في طي هذا التّقرير تشير إلى أن برمجيات التّجسّس، ومراقبة وسائل التّواصل الاجتماعي، والمراقبة بالتّعرف على الوجه—كلها تشكل قيودًا تطفّليّة على الوجود الفلسطيني وتُقلص حيّز الحياة المدنية في الأرض الفلسطينية المحتلّة، ففي الوقت الّذي تُطرح أنظمة وتقنيّات جديدة تحت مظلة تعزيز الأمن، تعمل هذه المُستجدات بخطىً ممنهجة لتغذية تآكل حق الفلسطينيين/ات في الخصوصيّة والتّجمع والحركة وحرية التّعبير. أدى نشر وتشريع أنظمة المراقبة التّوغليّة بلا قيدٍ أو شرطٍ على المدنيين/ات إلى خنق المجتمع المدني الفلسطيني مع تشديد الظّروف القمعيّة للحكم العسكري الإسرائيلي—الّتي تتجلّى في أولئك الذين يصمتون خشيةً من احتمال تنصّت جيش الاحتلال عليهم عبر هواتفهم المحمولة مرورًا بمن يسكنهم قلق اقتحام الجنود لمنازلهم لبناء تغذية لقاعِدة البيانات البيومترية. نظرًا لأن تطبيق المراقبة يشكل انتهاكًا منهجيًا للحقوق الأساسيّة للفلسطينيين/ات كما على النّحو المنصوص عليه في ميثاق الأمم المتحدة، فإن استخدام الجيش الإسرائيلي لتقنيات المراقبة على فئة المدنيين من الفلسطينيين/ات يتنافى مع جوهر القانون الدّولي ونصّه.

على هذه الجبهة، خَلُص خبراء قانونيّون ومنظّمات حقوقيّة كبرى إلى استنتاجات متشابهة، ففي تقرير نشرته اللجنة الدّولية للصليب الأحمر لعام 2020، تُشير اللجنة إلى أنّ أنظمة المراقبة الجديدة تطرح "قد تنثني تداعيات إنسانية" على المدنيين الذين يعيشون تحت الاحتلال العسكري، وتحديدًا من خلال «استهدافهم، واعتقالهم، وتعريضهم للإساءة والمعاملة القاسيّة أو المعاناة جرّاء الآثار النّفسية النّاجمة عن الخوف من كونهم تحت المراقبة."[73] وجدت منظمة العفو الدولية في الضّفّة الغربيّة بما فيها القدس الشّرقية المحتلّة أن توسّع المراقبة "يساعد تعزيز الأهداف الأمنيّة غير المشروعة للمستوطنين غير الشرعيين" من خلال تدعيم السّيطرة الإسرائيليّة على الفلسطينيين/ات وتقويض حقوقهم في الحركة، والتجمع، وحرية التّعبير.

---

65 المصدر السّابق.

66 Goodfriend, "Automated State Violence."

67 "الأبارتهايد الرقمي: تكنولوجيات التعرف على الوجه وترسيخ الهيمنة الإسرائيليّة." 2023.
https://www.amnesty.org/ar/documents/mde15/6701/2023/ar/

68 المصدر السّابق.

69 7amleh, "Intensification of Surveillance in East Jerusalem"

70 Shalhoub-Kevorkian, Nadera. 2015. Security Theology, Surveillance and the Politics of Fear. Cambridge Studies in Law and Society. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781316159927.11.

71 تحافظ شركة أوستو على شراكات مع حكومات ومؤسّسات في أمريكا الشّمالية وأوروبا الغربية. وفقًا لتقارير استقصائية أجراها موقع سيرفيلانس ديسكلوز (Surveillance Disclose)، فقد زودت الشّركة الناشئة الإسرائيليّة في مجال البيومتريا، بريفكام (Briefcam)، الشّرطة الفرنسية بكاميرات التّعرف على الوجوه سرًا لمدة ثماني سنوات. كما تُقدّم ترفد شركة كورسايت (Corsight AI) قوّات الشرطة بكاميرات محمولة مزودة بتقنية التعرف على الوجوه.

72 https://international-review.icrc.org/articles/ihl-hr-facial-recognition-technology-occupied-palestinian-territory-914

73 Committee for the Red Cross. 2020 "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centered Approach.» International Review of the Red Cross, Vol. 102, No. 913, 2020, p. 4.69

يمضي هذا التّقرير الموجز خطوةً أبعد ليبرهن على أنّ تطوير تقنيّات المراقبة ونشرها بلا قيدٍ أو شرطٍ في الأرض الفلسطينيّة المحتلّة لا يتعارض فقط مع مصالح السّكّان المدنيين الّذين يعيشون تحت حكمٍ عسكريٍّ يقرع عقودًا من الزمن؛ بل إنّه يضرّ أيضًا بالحقوق الأساسيّة للإنسان في كل مكان وأينما كان. إن الشّركات الإسرائيليّة الخاصّة تتجاهل القيود المترتبة على تنفيذ أنظمة المراقبة الرّقمية المدعّمة بتقنيّات الذّكاء الاصطناعي، من خوف، وقمعٍ، وانعدامٍ للأمان، كما هو الحال في الأرض الفلسطينية المحتلة وذلك في سبيل تسويقها وترويجها لتلك الأنظمة والتّكنولوجيا. في أسواق المراقبة والأمن العالمية، تسوّق برمجياتها للتجسّس، وتقنيّاتها لمراقبة وسائل التّواصل الاجتماعي وتِلك البيومترية كحلولٍ عامّة لانعدام الأمن الدّولي، حلولٍ جُرِّبت فعاليّتها واختُبِرت في إحدى أشهر بقاع النّزاع في العالم.

تُدلّل الفضائح الحقوقيّة الضّالعةِ بها الشركات الإسرائيليّة المشار إليها في هذه المذكرة على عدم فعالية تطوير ونشر هذه الأنظمة بل ومخاطرها على مستوى العالم أجمع ما لم تُنظّم كما ينبغي. كما في فلسطين، يسفر استخدام برمجيات التّجسس، ومراقبة وسائل التواصل الاجتماعي، وتقنيات التّعرف على الوجوه من مختلِف الحكومات في العالم عن تآكل الحق في الخصوصية، والحقّ في التجمع، والحقّ في الحركة، وحرية التّعبير. من آثار مجموعة اِن. اس. أو. المرعبة على الصحفيين/ات والمجتمع المدني وصولًا لتآكل العمليّات الديمقراطيّة بمساعدة شركات مراقبة وسائل التواصل الاجتماعي مثل فريق خورخي، لم تسهم هذه الأنظمة في تعزيز الأمان في أي سياقٍ طُبِّقت فيه، بل تسبّبت وتتسبب هذه التّقنيّات في مفاقمة العنف في بقاعٍ كثيرة العالم.

سادسًا. توصيات

يمكن لإسرائيل اتخاذ خطوات فوريّة لوقف الأضرار المُلحقة بالفلسطينيين/ات جرّاء تقنيات المراقبة الجديدة، بما في ذلك وقف بناء وتوسعة المستوطنات، وإنهاء المراقبة الجماعية للمدنيين الأبرياء، وإنهاء الرّصد والتّعقب القمعي للفضاءات الرقمية الفلسطينيّة. مركز حملة ليس بأول المنظّمات الحقوقيّة الكبرى الّتي تقدّم مثل هذه التّوصيات؛ لذا وفي ظل إحجام إسرائيل عن الالتزام بهذه الإرشادات، فضلًا عن الالتزامات المنصوص عليها بموجب القانون الدولي كما هو موضح آنفًا، فإنّه حري بالمجتمع الدّولي أن يتخذ خطواتٍ ملموسةٍ للحدّ من تطوير الشّركات الخاصّة ونشرها للتقنيات التّوغّليّة الجديدة.
يدعو مركز حملة دول العالم إلى وضع أُطرٍ قانونيّة شاملة مبنيةٍ على الحقوق لتنظيم استخدام وتطوير وإنتاج تقنيات المراقبة الآليّة والأسلحة، بالإضافة إلى آليات مساءلة للجهات الفاعلة من الشركات القائمة. يجب أن تركز هذه الأطر بشكل خاص على حماية خصوصية المدنيين وغيرها من حقوق الإنسان الأساسيّة. استلهامًا من تشريعات حماية البيانات المرعيّة لدى الاتحاد الأوروبي، مثل اللائحة العامّة لحماية البيانات، يمكن للدّول إنفاذ قوانين خصوصية تحدّد نطاق الأنشطة المسموح بها للمراقبة، والتّصريح بممارسات معالجة البيانات الشّفافة، وتمكين الأفراد من الحق في الوصول إلى بياناتهم الشخصية وتصحيحها ومحوها.[74] ستساعد هذه الضمانات القانونية في منع المراقبة العشوائيّة، بالتّوازي مع بناء المساءلة وضمان ملاءمة وضروريّة تدابير المراقبة وإخضاعها للإشراف والرقابة. يجب أن تواصل الهيئات الدولية، مثل الأمم المتحدة، دورها الرئيسي في تيسير التعاون للوصول لمعايير واتفاقيات عالمية مُركّزة على الحقوق بشأن الاستخدام المسؤول لتقنيات المراقبة، بالذّات في مناطق النزاع. علاوة على ذلك، وكخطوة مهمة نحو إنفاذ معايير احترام الحقوق والعرف الدولي، من الضروري محاسبة الجهات الفاعلة السيئة، التي تسببت في الضرر، على أفعالها وممارساتها التجارية فيما يتعلق بتقنيات المراقبة الضارة.

ضمن ذات الإطار والمسعى، ينبغي للدول تطبيق أُطُر قانونية شاملة لتنظيم بيع هذه التقنيات وتصديرها، حيث أنّ المطالبات بضرورة ضبط الحكومات لعمليات البيع هذه الأنظمة ونقلها في تزايد، بل قد لقيت تأييدًا من منظمات حقوق الإنسان الكبرى والهيئات الحاكمة، بما فيها الأمم المتحدة والصليب الأحمر.[75] ففي الوقت الّذي أقدمت فيه دول مثل الولايات المتحدة الأمريكية، على إدراج شركات مُسيئة على قوائمها السوداء، مثل مجموعة اِن. اِس. أو. وكانديرو، فإنّ تركيز الجهود على شركات معينة، دون فرض قوانين تنظيمية شاملة على الصناعة برمتها، قد يحد من المطلوب للتخفيف من الآثار الضّارة لهذه التّقنيّات. لذا، ينبغي للهيئات الدّولية فرض إطار عمل شامل وعالمي لتنظيم بيع ونقل هذه الأنظمة. علاوة على ذلك، يجب حظر بيع بعض التقنيات تمامًا. لقد توصل المجتمع الدولي في مناسبات عديدة إلى اتفاق على أن بعض الأسلحة تتعارض مع احترام الكرامة الإنسانية. ومع استمرار استخدام تقنيات المراقبة كسلاح، يبدو أننا نصل إلى حالة أخرى من هذا القبيل. يُمكن لهذه الخطوات تقديم نموذج لإسرائيل علّها تحذو حذوه، مع تقييد قدرة الشّركات الإسرائيلية، التي تستثمر في الاحتلال، على العمل بفعالية.

---

74 "General Data Protection Regulation (GDPR) – Official Legal Text." 2016. Accessed December 6, 2023. https://gdpr-info.eu/.
75 UN Affairs. 2023. "UN and Red Cross Call for Restrictions on Autonomous Weapon Systems to Protect Humanity | UN News." UN News. October 5, 2023. https://news.un.org/en/story/2023/10/1141922.