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

العرض والطّلب:

الأثر الأمريكي على قطاع المُراقبة الإسرائيلي

تموز/يوليو 2022

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

صوفيا چُدفْرِنْد

العرض والطّلب: الأثر الأمريكي على قطاع المُراقبة الإسرائيلي

مقدّمة

شهد مطلع عام 2022 موجةَ إدانة دوليّة لقطاع المراقبة الإسرائيلي عقب أنباء عن ممارساته التّعسفيّة الّتي تصدّرت عناوين الصّحف. آنذاك زعم ائتلاف من الصحفيين والصّحفيات ومنظمات المجتمع المدني أنّ برامج تجسّس إسرائيليّة استُخدِمت لاستهداف زهاء 50000 صحفي/ـة ومدافع/ـة عن حقوق الإنسان، عدا عن العديد من رؤساء الدّول.[1] في سياقٍ متصل، كشفت صحيفة واشنطن بوست أنّ الجيش الإسرائيلي نشر حشدًا من كاميرات التّعرف على الوجوه وقواعد البيانات البيومتريّة لمراقبة المدنيات والمدنيين من الفلسطينيين في الضّفّة الغربيّة، بل وتعاقد مع شركات خاصّة لتوسيع نطاق مراقبته.[2] إزاء هذه المُعطيات، يحذّر خبراء قانونيون دوليون أنّ تقنيات المراقبة الإسرائيليّة باتت تُهدّد حقوق الإنسان في مختلِف أنحاء العالم.[3]

---

[1] منظّمة العفو الدّوليّة. **تسرب هائل للبيانات يكشف عن استخدام برمجيات التجسس لمجموعة إن إس أو الإسرائيلية في استهداف النشطاء والصحفيين والزعماء السياسيين على مستوى العالم.** 9 تموز/يوليو 2021، تمّت مُعاينة المُحتوى في 12 أيّار/مايو 2022: https://www.amnesty.org/ar/latest/news/2021/07/the-pegasus-project/

[2] Hendel, Jonathan. 3 May 2022. "The watchful eye of Israel's surveillance empire" *972 Magazine.* Accessed 18 May 2022: https://www.972mag.com/israel-surveillance-facial-recognition/

[3] DeSombre, Winona. Lars Gjevik, and Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council.* Accessed 10 May 2022: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#conclusion

على حين أنّ الصحفيات/ين، والسّياسيين/ات ، والمدافعات/ين عن حقوق الإنسان غالبًا ما يصورون ماكينة المراقبة الإسرائيليّة على أنّها حالة استثنائية، إلّا أنّها لم تتطور بمعزل عن غيرها. يُفصّل هذا التّقرير تأثير الولايات المتحدّة على قطاع المراقبة الإسرائيليّة بين عامي 2002 و2022. وُضِعت نتائج البحث ضمن ثلاث نقاط أساسيّة: أولًا، يُحلّل التّقرير كيفيّة تطبيق إسرائيل لنموذج مراقبة بالتّعاون ما بين الدّولة والقطاع الخاص—جرى تطوير هذا النّموذج في الولايات المتحدّة في أعقاب أحداث 11 أيلول/سبتمبر من خلال التّعاون الرّسمي بين الأجهزة الأمنيّة في البلدين. ثانيًا، يبحث التّقرير في موقف الولايات المتحدّة المناهض لتنظيم شركات التكنولوجيا موضّحًا بالتفصيل كيف ضخّت شركات وجهات استثماريّة أمريكيّة ملايين الدّولارات في قطاع المراقبة المُتنامي في إسرائيل. أخيرًا، يسلّط البحث الضّوء على الآثار السّياسيّة لتأثير الولايات المتحدّة على قطاع المراقبة الإسرائيلي ويحدّد كيف يمكن للجهات التّشريعيّة الأمريكيّة وضع معايير تنظيميّة عالميّة. وعليه، يقدّم هذا التّقرير السّياق والتّحليل الأساسيَيْن للسجالات المُلحّة الّتي تُحيط بتطويع التّقنيات الجديدة وإساءة استخدامها.

نموذج مراقبة الشّركات والدّولة: من الولايات المتحدّة إلى إسرائيل

تعود انطلاقة قطاع المراقبة الإسرائيلي لأوائل العقد الأوّل من القرن الحادي والعشرين مع نموذج مراقبة الدولة والشركات (State-Corporate Surveillance) الرّائد في الولايات المتحدّة. تصف شوشانا زوبوف، عالمة الاجتماع في جامعة هارفارد، هذه الحقبة بـِ "فجر رأسماليّة المراقبة،" وتعرفها على أنّها نظام اقتصادي يدر الرّبح باستخدام البيانات الشّخصيّة لمستخدمي التّطبيقات التّكنولوجيّة.[4] تمكّن عمالقة التّكنولوجيا في الولايات المتحدّة—مثل Google، وMicrosoft، وApple، وMeta—الّذين تأسسوا للهيمنة على خدمات الاتصالات اللّاسلكيّة، من نيل نفاذ غير مسبوق إلى معلومات المستخدمين والمستخدمات الّتي عملوا على استغلالها لتدعيم قدرتهم على جمع وتحليل الاتصالات الخاصّة. في ظلّ شح اللّوائح النّاظمة لعملياتها غالبًا ما تُشارك هذه الشّركات التّكنولوجية بياناتها مع أجهزة الدّولة في الولايات المتحدة، الّتي لطالما جهدت لمواكبة الابتكارات المدنيّة.[5]

[4] Zuboff, Shoshanna. 2019. *The Age of SurveillanceCapitalism: The Fight for a Human Future at the New Frontier of Power.*Profile Books: New York.

[5] المرجع السّابق، 155.

يُشير جاك بالكين أستاذ القانون بجامعة ييل (Yale University) في بحثه بشأن سياسة الأمن القومي الأمريكيّة وتقنيات المعلومات الجديدة أنّه بحلول أواخر العقد الأوّل من القرن الحادي والعشرين، أصبحت شركات المراقبة العامّة والخاصّة في الولايات المتحدة متواشجة ومتشابكة،[6] إذ أن أحداث الحادي عشر من أيلول/سبتمبر وما تلاها من حرب على الإرهاب وما زامن ذلك من تصاعد للاقتصاد الرّقمي جميعها دفعت وكالات الاستخبارات العامّة وشركات الإنترنت الخاصّة إلى بناء شكل من الاحتياجات التّكامليّة فيما بينها. وعليه، ضخّت الحكومةُ الأمريكيّة، وتكتلات الشّركات، والشّركات التّكنولوجيّة النّاشئة الموارِدَ اللّازمة لتطوير تقنيات مراقبة متقدمة بُغية حصد بيانات المستخدمين والمستخدمات. شمل ذلك أدوات المراقبة الجماعيّة، مثل تقنية التّعرف على الوجه، واستخراج البيانات من وسائل الإعلام اجتماعي (Social Media Scrabbing)، بالإضافة إلى الرّصد والمتابعة الموجّهة—بما في ذلك برامج التّجسس وأجهزة تشويش إشارة الإرسال. هكذا قدّمت الشركات الخاصّة الأدوات والخبرات إلى الحكومة مقابل القليل من الرقابة التنظيمية على عملها. إنَّ موقف الولايات المتحدّة المناهض للتنظيم جعل من الإنترنت والتّقنيات المطورة لمراقبته فضاءً لا قانون فيه، كما يصفه الخبراء.[7]

اقتفت العديد من البلدان النّموذج الأمريكي للمراقبة القائم على الشّراكة بين المزاوجة بين أجهزة الدّولة والشّركات الرّبحية الخاصّة؛ أمّا إسرائيل، فلم تكن استثناءً، فهي المتلقي الأكبر للمساعدات الأمريكيّة المتراكمة منذ الحرب العالميّة الثّانية والحليف المُقرّب للولايات المتحدة.[8] بدءًا من أوائل العقد الأوّل من القرن الحادي والعشرين، تباحث رؤساء أجهزة المخابرات الإسرائيليّة مع خبراء الأمن الأمريكيين والرّؤساء التّنفيذيين للشركات التّكنولوجيّة بهدف تعظيم أوصال جهاز المخابرات الإسرائيلي في الأراضي المحتلّة (الضّفة الغربيّة، والقدس الشّرقيّة، وقطاع غزّة) لتلبية متطلبات العصر الرقمي.[9] هكذا نمت وحدات مثل وحدة 8200—النّسخة الإسرائيليّة من وكالة الأمن القومي الأمريكي—من وحدات استخبارات إشارة غير فاعلة إلى

[6] Balkin, Jack. 2008. "The Constitution in the National Security State." *Minnesota Law Review.* Accessed 17 May 2022. https://openyls.law.yale.edu/handle/20.500.13051/1545
[7] N.A. "The Wild West of Smart Phone Data." 2021. *Council on Foreign Relations.* Accessed 17 May. 2022. https://www.cfr.org/blog/wild-west-smartphone-data-and-surveillance
[8] N.A. 2022. "U.S. Foreign Aid to Israel." Congressional Research Service. Accessed 10 May 2022. https://sgp.fas.org/crs/mideast/RL33222.pdf.
[9] IMEU. (2021, November 29). Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement | IMEU. Institute for Middle East Understanding (IMEU). Retrieved May, 2022, from https://imeu.org/article/fact-sheet-israeli-surveillance-restrictions-on-palestinian-movement

ما وصفه جنرالات بـ"تجمّع من الشّركات الصغيرة الناشئة"[10] يضم في صفوفه جنودًا أكثر من البحريّة الإسرائيليّة."[11] بدأ الجيش بتدريب مجنديه ومجنداته الشّباب على القرصنة الهجوميّة، وتطوير التّطبيقات التكنولوجيّة، وتحليل البيانات. تُشير الأبحاث إلى أنّ وحدّات المخابرات الإسرائيليّة أظهرت قدرتها على برمجة تقنيات متطورة لمراقبة المدنيين والمدنيات الفلسطينيين الّذين يقبعون تحت الاحتلال ويُحرمون من حقّهم بحماية خصوصيتهم كل يوم باسم المخاوف الأمنيّة الإسرائيليّة.[12] في المقابل، اكتسب الجنود الإسرائيليون خبرة عملية في بناء وإدارة تقنيات المراقبة والأمن الجديدة باعتبارها جزء من خدمتهم العسكريّة وكانوا متحمسين لحمل ما في جعبتهم من تقنيات ومهارات جديدة إلى القطاع الخاص بمجرد تسريحهم من الخدمة.

أدّى توسّع جهاز المراقبة العسكريّة الإسرائيليّ في الضّفة الغربيّة إلى رَفد التّطور السّريع لاقتصاد التّكنولوجيا المتقدّمة في إسرائيل. معولةً على العلاقات الوثيقة بين الجيش وقطاع التّكنولوجيا الخاص الّتي تأسّست قبل عقود،[13] شهد قطاع التكنولوجيا في إسرائيل نموًا غير مسبوق في أعقاب أحداث الحادي عشر من أيلول/سبتمبر حيث ارتفع الطّلب على تقنيات الأمن والمراقبة في جميع أنحاء العالم.[14] بالمثل وبقيادة قدامى وحدات الاستخبارات العسكريّة الإسرائيليّة، انتشرت ونمت الشّركات النّاشئة الإسرائيليّة الّتي عكفت تُجرّب وتستكشف مكامن تقنيات الذّكاء الاصطناعي، وتحليل البيانات، والتّجسس الإلكتروني. في المحصّلة، بات للتحالفات بين إسرائيل والولايات المتحدة معنى مفاده أنّ الجيش الأمريكي، و وكالة المخابرات المركزية الأميركية "سي آي إيه" (CIA)، ومكتب التحقيقات الفيدرالي باتوا عملاء دائمين لشركات المراقبة الإسرائيليّة.[15] بحلول عام 2016، كانت إسرائيل مرتعًا لمعظم شركات المراقبة لكل فرد في العالم وتعتبر "عاصمة الأمن الدّاخلي" العالمية.[16]

---

[10] Bar, Eli, Gabi Ayalon, Amnon Angor, and Zvi Fishler. "8200 State of Being: DNA or an Organizational Culture?" *Migdalor*. June 2007. (Hebrew)

[11] Adler, Seth. "Inside the Elite Israeli Military Unit 8200." *CyberSecurityHub*. 11 June 2020. Accessed 10 May 2022. https://www.cshub.com/threat-defense/articles/inside-the-elite-israeli-military-unit-8200

[12] Talbot, Rohan. 2021. "Automating Occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory." *International Review of the Red Cross*. 102.914 (823-849).

[13] Maggor, Erez. 2020. "The Politics of Innovation Policy: Building Israel's 'Neo-Developmental State.' *Politics & Society*. (1-37)

[14] Gordon, Neve. 2010. "Israel's Emergence as a Homeland Security Capital". *in Surveillance and Control in Israel/Palestine. Population, Territory and Power*. Ed. Elia Zureik, David Lyon, Yasmeen Abu-Laban. London: Routledge Press).

[15] Greenwald, Glen.. "Cash, Weapons, and Surveillance: The U.S. Is a Key Party to Every Israeli Attack." The Intercept. 4 April 2014. Accessed March 31, 2022. https://theintercept.com/2014/08/04/cash-weapons-surveillance/.
Greenwald, Glenn, Laura Poitras, and Ewen MacAskill. 2013. "NSA Shares Raw Intelligence Including Americans' Data with Israel." *The Guardian*. https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[16] N.A. "The Global Surveillance Industry." *Privacy International*. 2016. Accessed 17 May 2022. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

العرض والطلب

ساعد نهج عدم التّدخل الّذي اتبعته الولايات المتحدة في تنظيم تكنولوجيا المراقبة في جعل صناديق رأس المال الاستثماري والتكتلات التكنولوجيّة الّتي تتخذ من الولايات المتحدة مقراً لها من أكثر الممولين إنتاجًا لشركات المراقبة الإسرائيليّة الخاصة.[17] تعد Meta وMicrosoft، وGoogle، وAmazon، وApple نماذج أعمال رائدة تعتمد على التّتبع المستمر لمستخدمي ومستخدمات تطبيقاتها التّكنولوجيّة حتّى عند عدم اتصالهم/ن بالإنترنت. إلى الآن، استحوذت هذه الشرّكات على أكثر من 20 شركة إسرائيليّة مكرّسة لجمع أو تحليل البيانات الجماعيّة والمراقبة الموجّهة،[18] بما في ذلك الشّركات الّتي تسوق تقنيات المراقبة البيومتريّة، والتّجسّس الإلكتروني، وجمع البيانات.[19] إن الطّلب على تكنولوجيا مراقبة أكثر تعقيدًا يعني ضخ ملايين الدّولارات—من الشّركات الّتي تتخذ من الولايات المتحدّة الأمريكيّة مقرًا لها—إلى شركات المراقبة الإسرائيليّة النّاشئة. ومن بين هذه الجهات الاستثماريّة الأمريكيّة البارزة: فرانسيسكو بارتنرز (Francisco Partners)، الّتي تمتلك أسهم مجموعة ان اس او (NSO Group)؛[20] وباتري فنتشرز (Battery Ventures)، أحد ممولي شركة برامج التّجسس الإسرائيلية باراغون (Paragon)؛[21] وأندرسن هورويتز (Andressen Horowitz)، الّتي أسفرت استثماراتها عن إطلاق شركة توكا (Toka) للعلوم العدليّة الرّقميّة الإسرائيليّة؛[22] وشركة لايت-سبِيد فنتشرز (LightSpeed Ventures)، الّتي تمتلك أسهمًا في شركة القياسات البيومتريّة (Oosto) الّتي عُرفت سابقًا باسم انِي فِجِن (AnyVision).[23]

---

[17] Kortum, S., & Lerner, J. (2000). Assessing the Contribution of Venture Capital to Innovation. The RAND Journal of Economics, 31(4), 674–692. https://doi.org/10.2307/2696354

[18] N.A. "Aquisitions by Google"; "Acquisitions by Meta"; "Aquisitions by Microsoft."; "Acquisitions by Amazon" and "Acquisitions by Apple." *Tracxn*. N.D. Accessed 5 June 2022. https://tracxn.com/?redirect=false

[19] Christiansen, Siri. "Why All Investors Should be Concerned About Surveillance Technology." *CityWire*. 12 April 2022. Accessed 19 May 2022.
https://citywireselector.com/news/why-all-investors-should-be-concerned-about-surveillance-technology/a2384740

[20] Gilead, Asaf. "Squabbling Threatens NSO Sales." *Globes*. 29 Mar 2022. Accessed 5 May 2022.
https://en.globes.co.il/en/article-squabbling-threatens-15b-sale-of-nso-group-1001407395

[21] Brewster, Thomas. "Israeli Surveillance Startup That 'Hacks WhatsApp and Signal." *Forbes*. 29 July 2021. Accessed 5 May 2022.
https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/?sh=7d5832e3153b

[22] المصدر السّابق.

[23] N.A. "Lightspeed Venture Partners Invest in AI Leader to Accelerate Global Expansion." 14 January 2019. *Oosto*. Accessed 10 May 2022.

على حين أنّ العديد من شركات المراقبة الإسرائيليّة تصنّف نفسها على أنّها شركات مدنيّة، فإنّ أنشطتها تتأرجح بشيء من الزّئبقيّة بين السّياقات العسكريّة والمدنيّة. في السّنوات الأخيرة، تعرضت تقنيات ما يُعرف بالمراقبة "المزدوجة الاستخدام" لانتقادات لاذعة من المدافعين/ـات الحقوقيين/ـات والمشرعين/ات، الّذين يشدّدون على تحدي ضمان عدم استخدام الجيوش أو الأنظمة القمعية لتكنولوجيا المراقبة.[24] على سبيل المثال، إن شركة Oosto (المعروفة سابقًا بـAnyVision)، الّتي تم نصب كاميراتها للتعرف على الوجه عند نقاط التّفتيش الرّئيسة للجيش الإسرائيلي في الضّفة الغربيّة، تبيع الكاميرات البيومتريّة إلى "المدن الذّكية" في الولايات المتحدة. جدير بالذّكر أن شركة Microsoft كانت إحدى الجهات الممولة الرّئيسة للشركة النّاشئة في عام 2019 قبل أن تسحب استثماراتها بعد تقارير استقصائيّة كشفت عن مدى تعاون هذا الضّرب من الشّركات مع الجيش الإسرائيلي—بما في ذلك تركيب كاميرات التعرف على الوجه في الضّفة الغربيّة والقدس.[25] على الرغم من سحب Microsoft استثماراتها، تواصل Oosto تزويد الجيش الإسرائيلي بتقنية التّعرف على الوجه وتصدير تقنيتها إلى البلديات في أكثر من 40 دولة.[26]

على تُواصل الشركات الخاصّة مثل Oosto في جذب الملايين من المستثمرين رغم ما تلقاه من إدانة عامّة، يمضي السيليكون ڤالي (Silicon Valley) جهوده للسيطرة على قطاع المراقبة الذي لعب دورًا كبيرًا في تشكيله. إن صعود وسقوط مجموعة ان اس او (NSO Group)، وهي شركة تجسس إلكترونية إسرائيليّة يُزعم أنّها اخترقت هواتف 50000 من الصحفيين/ـات والمعارضين/ـات السياسيين/ـات والسياسيين/ـات طوال فترة نشاطها، يقدّم مثالاً واضحًا على ذلك. عملت مجموعة ان اس او (NSO Group) بشكل وثيق مع Silicon Valley طيلة معظم فترة عملها: تجري شركة Meta محادثات لشراء برمجيات تجسس من مجموعة NSO، على أمل استخدام برنامجها لمراقبة مستخدمي نظام تشغيل iOS للهواتف المحمولة في عام 2017.[27] بعد ذلك بعامين، عادت شركة Meta أدرجها لتقاضي الشركة الإسرائيليّة لنفاذها إلى خوادم تطبيق

---

[24] Gildea, Ross James and Federica D'Alesandra. "We Need International Agreement on How to Handle These Dangerous Technologies. *Slate.com.* 7 March 2022. Accessed 17 May 2022. https://slate.com/technology/2022/03/dual-use-surveillance-technology-export-controls.html

[25] Solon, Alina. "Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?" *NBCnews.com.* October 29, 2019. Accessed 10 March 2022.

[26] Hempel, Jonathon. "The Watchful Eye of Israel's Surveillance Empire." *972 Magazine.* 3 May 2022. Accessed 17 May 2022. https://www.972mag.com/israel-surveillance-facial-recognition/

[27] Holmes, Aaron. "Facebook is Suing an Israeli Spyware Company." *Business Insider.* 3 April 2020. Accessed 10 May 2022. https://www.businessinsider.com/nso-group-facebook-buy-pegasus-spyware-lawsuit-2020-4

WhatsApp لتثبيت برنامج Pegasus، وهو أحد العلامات التّجاريّة لمجموعة NSO، على الأجهزة المحمولة المستهدفة بالتّجسّس والتّتبّع. حذت شركة Apple حذوها في تشرين الثّاني/نوفمبر 2021، حيث أعلنت عن دعوى قضائية أقامتها على الشركة بعد فترة وجيزة من الكشف عن اختراق الشركة لهواتف مسؤولي/ـات وزارة الخارجية الأمريكية في أوغندا.[28] بمجرد تلقي الأخبار من Apple، وضعت وزارة التجارة الأمريكية مجموعة NSO وشركة برامج التجسس الإسرائيلية Candiru، إلى جانب أربع شركات مراقبة أخرى، في قائمة سوداء وحظرت تعامل هذه الشركات مع أي كيانات أمريكية. إلى جانب دعاوى Meta وGoogle رفيعة المستوى، أسفر إدراج شركة NSO في القائمة السّوداء في الولايات المتحدة إلى الدّفع بالشّركة من حافّة الإفلاس. وردت وزارة الدفاع الإسرائيلية بتشديد لوائح التصدير، وأجبرت شركة مراقبة خاصة واحدة على الأقل على الإغلاق.[29]

على الرغم من هذه التّطورات، يوضّح انهيار مجموعة NSO حدود المحاولات التّنظيميّة لهذا القطاع، فمجموعة NSO ليست سوى واحدة من مئات شركات برمجيات التّجسس الخاصّة الّتي تبيع أسلحة تجسس توغلية من الدّرجة العسكريّة للحكومات في جميع أنحاء العالم. في سياقٍ متصل، تقوم شركات مثل Dark Matter—مقرها الإمارات العربية المتحدة—بتوظيف أفراد من وكالات المخابرات الأمريكيّة أو الإسرائيليّة، وتَعِد برواتب ومزايا مجزيّة.[30] تقوم شركات برامج التجسس الإسرائيليّة الأخرى بالتّسجيل ببساطة في البلدان الّتي لديها قوانين تصدير متساهلة، مثل قبرص أو مقدونيا الشماليّة.[31] توضّح هذه التّوجهات كيف أن السّياسات الّتي تستهدف الشرّكات بشكلٍ فردي لا تجدي الكثير من النّفع، لا سيّما للحد من الممارسات التّعسفيّة لقطاع المراقبة الخاص. عِلاوة على ذلك، تواصل تكتلات الشّركات مثل Meta وGoogle الاستثمار في تقنيات المراقبة الاختراقيّة—لا سيّما تقنيات التّعرف على الوجه وجمع البيانات الّتي تم توثيق إساءة استخدام الحكومات

[28] Bergman, Ronen and Mark Mazetti. 28 January 2022. "The Battle for the World's Most Powerful CyberWeapon." *New York Magazine.* Accessed 15 April 2022.
https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
[29] Gilead, Assaf. "Export Controls Strangling Israel's Attack Industry." *Globes.* 25 April 2022. Accessed 17 May 2022.
https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066
[30] Mazzeti, Mark, Adam Goldman, Ronen Bergman, and Nicole Perlroth. "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments." *The New York Times.* 21 March 2019. Accessed 18 May 2022.
https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html
[31] Benjakob, Omar. 19 April 2022. 'Great Alarm': First Detected Use of Mysterious Israeli Spyware on EU National.' *Haaretz.* Accessed 10 May 2022.
https://www.haaretz.com/israel-news/tech-news/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter-1.10748821

والشركات الخاصّة لها. على الرّغم من الإعلان عن التزام جديد بتضييق الخناق على قطاع المراقبة،[32] تلعب هذه الشّركات دورًا محوريًا في تمويل تقنيات المراقبة دون أي مساءلة أمام مستخدميها أو الرّقابة التنظيميّة من قبل الهيئات المحليّة أو الدوليّة.

الخلاصة

يوضح هذا التّقرير بالتّفصيل تأثير السّياسات الأمريكيّة وممارسات الشّركات على قطاع المراقبة الإسرائيلي: حيث أسفر التّعاون بين السيليكون ڤالي (Silicon Valley) والحكومة الأمريكيّة عن إتاحة المجال للتكتلات التكنولوجية ورؤوس المال الخاصّة للاستثمار في برمجيات مراقبة توغليّة دون حسيب أو رقيب. منذ أوائل العقد الأوّل من القرن الحادي والعشرين، تهافتت الشّركات الإسرائيليّة النّاشئة لسد الطّلب المتزايد على وسائل أكثر ابتكارًا لمراقبة وتتبع النّاس. إذ عمِد العديد من مؤسّسي هذه الشّركات لاستخدام أنظمة المراقبة ولمعرفة الكيفيّة التكنولوجية الّتي تم تطويرها في الجيش الإسرائيلي للمراقبة الجماعية للمدنيين/ـات المحرومون من حقّهم في حماية خصوصياتهم. في المقلب الآخر، أقدمت تكتلات شركات التكنلوجيا وصناديق التّحوط الّتي تتخذ من الولايات المتحدة مقراً لها والتي تعمل دون أي حسيب أو رقيب على شراء هذه التقنيات التجسّسية التّوغليّة؛ حيث يوفّر طلب هذه الجهات لهذه البرمجيات الأرضيّة اللّازمة لصناعة برمجيات المراقبة الخاصة العالمية. وعلى حين أنّ هذه الشّركات ذاتها تقود جهود السّيطرة على صناعة تقنيات المراقبة، فإنّ الحلول الّتي يقدّمها القطاع محدودة. إزاء هذا الواقع، ينبغي للولايات المتحدّة والمنظمات الدّولية بذل المزيد من الجهود لضمان حماية فعّالة للخصوصية بالإضافة إلى وضع القيود اللّازمة على بيع تكنولوجيا المراقبة ونقلها.

التّوصيات:

تمتلك المؤسّسة الأمنيّة الأمريكيّة وشركات التكنولوجيا الّتي تتخذ من الولايات المتحدة مقراً لها نفوذًا هائلًا على قطاع المراقبة الإسرائيلي، ما يعني أنّ الولايات المتحدة لديها القدرة على الإسهام في وقف الممارسات المسيئة الّتي تعتري هذه الصّناعة. وعليه يجب على الولايات المتحدة سَن أنظمة شاملة ومُمتدّة الأثر لتنظيم بيع ونقل تقنيات المراقبة الجماعية والموجهة. إلّا أن الكونجرس الأمريكي قد فشل، إلى الآن، في تمرير تشريع واحد شامل لحماية مستخدمي/ـات التكنولوجيا

[32] Dvilanski, Mike, David Agranovich, and Nathaniel Gleicher. December 2021. "Threat Report on the Surveillance-for-Hire Industry." *Meta.* Accessed 17 May 2022. https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

وتنظيم تكتلات شركات البرمجيات التكنولوجيّة.[33] لذا فإن وجود تشريع يحظر المراقبة الجماعية العشوائية من قبل الكيانات العامّة والخاصّة على حد سواء، ويضع قيودًا على جمع البيانات من قبل شركات التّطبيقات والبرمجيات التكنولوجية إلى جانب تكريس شموليّة الحق في الخصوصيّة على المستوى الفيدرالي بات أكثر إلحاحًا من أي وقت مضى، حيث ستعمل مثل هذه السّياسات على كبح الطّلب على برمجيات المراقبة الأكثر توغلًا وبالتّالي تقليل الاستثمارات الخاصّة في الشرّكات الجديدة العاملة في هذا المضمار.

بالإضافة إلى القوانين الفيدرالية، حري بالولايات المتحدّة الأمريكيّة الانضمام إلى الجهود الرّامية لوضع أنظمة دوليّة واسعة وشاملة بشأن بيع ونقل تقنيات المراقبة في جميع أنحاء العالم. على حين تبيع شركات المراقبة الخاصة منتجاتها في جميع أنحاء العالم—دون تمييز بين الحكومات الديمقراطية وتكتلات الشّركات والأنظمة القمعية —دعت الأمم المتحدة وتحالف واسع النطاق من منظمات المجتمع المدني إلى وضع سياسات شاملة تحد من استخدام هذه التّقنيات والاتجار بها.[34] من الواضح أنّ القيود المفروضة على بعض الأسلحة السيبرانية، مثل إدراج شركتي Candiru ومجموعة NSO على القائمة السوداء في لولايات المتحدة، لن تحد من المخاطر الّتي تشكلها تقنيات المراقبة الأخرى الّتي تعمل بالذكاء الاصطناعي، مثل تقنية التعرف على الوجه وتعقّب الموقع؛ لذلك، من لا بدّ أن توقع كافّة الحكومات على نظام ملزم وشامل للرقابة على الصادرات يفرض قيودًا دائمة على منتجات المراقبة، لا سيّما تقنيات المراقبة الّتي تعمل بالذكاء الاصطناعي. طالبت الأمم المتحدة بدوها أن تضمن هذه الضوابط التزام شركات المراقبة بالمبادئ التوجيهية للأمم المتحدة بشأن الأعمال التجارية وحقوق الإنسان، لما توفره من آلية مهمة لمساءلة الشركات.[35] من خلال الانضمام إلى الجهود الرّامية لوضع إطار عمل تنظيمي دوليٍّ ناظم لبرمجيات المراقبة، يمكن للولايات المتحدة منع الشّركات الجديدة في إسرائيل وخارجها من تطوير تقنيات أكثر توغلًا.

يقدّم النّضال من أجل الحقوق الرقميّة في فلسطين شواهد على المخاطر الّتي تشكلها المراقبة غير المنظمة في جميع أنحاء العالم. في هذا السّياق، وثّق مركز حملة كيف أن استخدام إسرائيل غير المنظَّم لأنظمة كاميرات المراقبة، وأدوات

[33] Kang, Cecilia. "As Europe Approves New Tech Laws the U.S. Falls Behind." *The New York Times*. 22 April 2022. Accessed 5 June 2022. https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html
[34] N.A. "Spyware: Rights experts push for surveillance technology moratorium." *UN News: The United Nations*. Accessed 18 May 2022. https://news.un.org/en/story/2021/08/1097632
[35] Keaten, Jamey and Matt O'Brien. "U.N. urges moratorium on use of AI that imperils human rights." *The LA Times*. 16 Sept 2021. Accessed 5 June 2022.
https://www.latimes.com/business/story/2021-09-16/u-n-urges-moratorium-on-use-of-ai-that-imperils-human-rights

المراقبة البيومترية، والمراقبة المكثفة لوسائل الإعلام الاجتماعي يقيّد حرية الفلسطينيين والفلسطينيات في التّعبير وحريّة التّنقل والحق الأساسي في الخصوصية.[36] تُشير الأبحاث أنه على حين يعكّف المسؤولون الإسرائيليون على تصوير تقنيات المراقبة الجديدة كحلول أمنية إنسانيّة، فإن هذه الأنظمة تسبب أضرارًا نفسية كبيرة وتعتمد على ممارسات شرطية ذات أبعاد توغليّة وتدخليّة.[37] لذا وفي ضوء كل ما تقدّم، يجدر بصانعي/ـات السياسة في الولايات المتحدة أن يطبّقوا مبادئ المساءلة على قطاعٍ أفلت من العقاب لفترة طويلة جدًا، يُمكن لذلك أن يبدأ بجُملة من التّغيرات في الأنظمة والسّياسات، فضلاً عن ضرورة التزام الشرّكات ورؤوس الأموال الاستثماريّة الأمريكيّة بالتوقف عن استنهاض صناعة المراقبة الخطرة، واتخاذ خطوات ملموسة للسيطرة على هذا السّوق.

[36] 7amleh. "Intensification of Surveillance in East Jerusalem and Impact of Palestinian Residents' Rights."*7amleh: The Arab Center for Social Media Advancement.*
https://7amleh.org/2021/11/08/intensification-of-surveillance-in-east-jerusalem-and-impact-on-palestinian-residents-rights-summer-and-fall-2021

[37] Goodfriend, Sophia. 21 February 2022. "How the Occupation Fuels Tel Aviv's Booming AI Sector." *Foreign Policy.* Accessed 10 May 2022. *https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/* and Shtaya, Mona. "Nowhere to Hide: The Impact of of Israel's Digital Surveillance Regime on Palestinians. The Middle East Institute. Accessed 5 June 2022.
https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians