

وَقَع السَّيَّاسَات الإِسْرَائِيلِيَّة عَلَى حَقُوق الفِلَسْطِينِيِّين الرِّقْمِيَّة خِلَالَ تَفْشِي فَيروس كورونَا المَسْتَجِدِّ

د. نجمة علي *

في محاولة للتصدي لجائحة فيروس كورونا، تستخدم دول عديدة حول العالم اليوم، وبشكل متزايد، تقنيات خطيرة على حساب حماية حقوق الإنسان الأساسية. وفي آذار/ مارس 2020، صادقت الحكومة الإسرائيلية على تشريعي طوارئ جديدين¹، يهدفان إلى غايتين، الأولى؛ فرض قوانين عزل اجتماعي جديدة. أما الثانية؛ تتبّع المرضى المصابين بالفيروس. وألقيت المهمة على عاتق جهاز المخابرات الإسرائيلي الداخلي ("الشاباك"). وقبول ذلك باستجابة غاضبة من ناشطي الخصوصية خاصة، وحقوق الإنسان عامة، لكون التشريعين الجديدين عبارة عن توسيع لاستخدام الحكومة الإسرائيلية لتقنيات المراقبة الجماعية، وخاصة تلك التي يُشرف عليها "الشاباك"، مما يُعدّ انتهاكاً إضافياً لحقوق الرقمية وحقوق الإنسان.

ويهدف هذا التقرير إلى توثيق كيف نشرت إسرائيل تقنيات المراقبة الجماعية خلال جائحة فيروس كورونا، وتقصّي أثر هذه السياسات والممارسات على حقوق الفلسطينيين الرقمية؛ أي الحق في الخصوصية، وحرية التعبير، وحماية البيانات. كما ويكشف إطار الأمنة الذي تعالج فيه الحكومات الأزمة الصحية العالمية، أي كيف خلق تفشي فيروس كورونا فرصة للدول والحكومات لتأطير سياسات وممارسات تحت خانة "الضرورة الأمنية"، مما أدى ويؤدي إلى توسيع نطاق المراقبة الشاملة، وخلق مناخ متقبل إلى حدّ التعايش الطبيعي مع هذه الممارسات في فترات الأزمات.

يستند هذا التقرير إلى مقالات صحافية، وأكاديمية، وكتب، بالإضافة إلى أوراق موقف وتصريحات صادرة عن منظمات من المجتمع المدني. ويبدأ بالتمعن في هيكلية منظومة المراقبة الرقمية الإسرائيلية، ومن ثمّ يصبّ تركيزه على المراقبة الحكومية خلال فترة انتشار فيروس كورونا، مستعرضاً قوانين المراقبة الرقمية التي تبنتها الحكومة الإسرائيلية، وآثارها المترتبة على الحقوق الرقمية. ويحدّد المقطع الثالث تقنيات المراقبة الشاملة التي استُخدمت لمكافحة فيروس كورونا، ويسلّط الضوء على المضاعفات السلبية التي قد تسببها هذه التقنيات، على الحق في الخصوصية وحماية البيانات لجميع الأفراد الذين يعيشون في إسرائيل والمناطق الفلسطينية المحتلة، بما في ذلك اليهود الإسرائيليين، متطرقاً أيضاً لنمط استخدام هذه التقنيات للاستهداف المنهج لمجموعات سكانية معينة. ناهيك عن أنّ اعتماد استراتيجيات المراقبة الشاملة يثير قضية

¹ Library of Congress Law- Global legal Monitor. (2020). Israel: Emergency Regulations Authorize Digital Surveillance of Coronavirus Patients and Persons Subjected to Home Isolation. Retrieved from: <https://www.loc.gov/law/foreign-news/article/israel-emergency-regulations-authorize-digital-surveillance-of-coronavirus-patients-and-persons-subjected-to-home-isolation/>



السياسات التمييزية التي تفضح "الوجه التكنولوجي" للقمع الإسرائيلي. نهاية، وفي سبيل حماية الحقوق الرقمية في إسرائيل والمناطق الفلسطينية المحتلة، تقدم ورقة الموقف توصياتها لضمان حيز رقمي حر، وآمن، وعادل للجميع؛ لا سيما لجماعات اجتماعية، وقومية، وعرقية وسياسية محددة، كالفلسطينيين مواطني إسرائيل، والفلسطينيين في المناطق الفلسطينية المحتلة عام 1967.

1. هيكلية منظومة المراقبة الرقمية الإسرائيلية

تعدّ التقنيات الحديثة للمراقبة الرقمية، أو مراقبة شبكات الاتصالات، عملية استخباراتية صُممت من أجل جمع المعلومات الرقمية، والاحتفاظ بها، ومعالجتها، ومن ثمّ تحليلها، عبر الحصول عليها من شبكات الاتصالات الإلكترونية؛ أي الخطوط الأرضية، والشبكات الخليوية، والإنترنت أو شبكات البيانات المختلفة. وتبدأ المراقبة باعتراض المعلومات واستخراجها من الشبكة، وجمع بيانات الاتصالات، ومقدمي خدمة الاتصالات أو شركاتها، ومعالجة معلومات مكشوفة ومخبأة والتي قد تتضمن أساليب "التنقيب في البيانات"².

في زمن تُدار فيه اتصالات ضخمة بين البشر عبر الوسائط الإلكترونية، تستطيع السيطرة على التكنولوجيا الحديثة من أجل جمع البيانات على نطاق واسع، وتخزينها وتحليلها إحصائياً، أن تمنح صاحبها القدرة على تحصيل معلومات استخباراتية أكثر تفصيلاً وإنتاجية، عن المستهدفين في عملية المراقبة، بشكل أكبر من أي زمن آخر. ومع ذلك، فإنّ هذا بمثابة سيف ذو حدين عندما يتعلق الأمر بحقوق الإنسان وانتهاك الخصوصية وحماية البيانات، عند الأخذ بعين الاعتبار، أنّ المراقبين ليسوا وحدهم من يتعرّض للاستهداف، بل أولئك الذين على اتصال بهم أو تواصل معهم أيضاً. وهناك عنصر إضافي يرتبط بالأذى الذي يلحق بالأفراد من جراء المراقبة الرقمية، وهو لا يقتصر على انتهاك حقهم بالخصوصية فقط. فعند النظر إلى نطاق أوسع، يمكننا أن نرى أنّ تبعات ممارسات المراقبة المماثلة قد تضرّ بإحساس الأفراد المستهدفين بالحرية، وحرية التعبير.³ فعندما يعي الأفراد أنّهم مراقبون، أو أنّهم قد يكونون كذلك، فمن المرجح أن يعدّلوا سلوكياتهم تبعاً، ممّا يُضخّم إحساسهم الداخليّ بالرّقابة. ومنذ أعوام طويلة، تستخدم إسرائيل المراقبة الشاملة لملاحقة الفلسطينيين في المناطق الفلسطينية المحتلة وإسرائيل، ولكّنها، وتحت وطأة انتشار فيروس كورونا المستجدّ، وجّهت تقنيّاتها المتطورة لتتبع مواطنيها اليهود أيضاً، وعلائيّة. مع ذلك، يكشف القسم التالي أنّ إسرائيل تراقب مواطنيها قبل انتشار الفيروس بكثير.

² The Israel Democracy Institute. (2019). Regulation of Online Surveillance on Israeli Law and Comparative Law. Retrieved from: <https://en.idi.org.il/media/13042/regulation-of-online-surveillance-final.pdf>

³ Ibid



1.1 تَأْصِيل الرِّقَابَة الرِّقْمِيَّة فِي إِسْرَائِيل، وَانْتِهَاكَات حَقُوق الْإِنْسَان

تقدّم إسرائيل نفسها بوصفها دولة تتمتع بتشريعات مختلفة تغطّي الحقّ في الخصوصية، بما في ذلك المادة السابعة من قانون الأساس حول كرامة الإنسان وحرّيته؛ وقانون حماية الخصوصية؛ ومسجّل قواعد البيانات؛ وقانون خدمة بيانات الائتمان؛ وقانون المراقبة السريّة (1979)؛ وقانون الحواسيب (1995)؛ وقانون المعلومات الجينيّة؛ وقانون حرّية المعلومات. بناء على ما سبق، تعتبر المفوضية الأوروبيّة أنّ قوانين حماية البيانات الإسرائيليّة تقدّم مستوى كافٍ من حماية البيانات الشّخصيّة المتنقّلة بين دول الاتّحاد الأوروبيّ.⁴ يقدّم حلبي⁵ نظرة نقدية للتشريعات الأمنيّة الإسرائيليّة، والتي توفّر مراجعة مفصّلة لتقنيّات المراقبة وممارساتها، والتي تطبّقها إسرائيل على مواطنيها؛ كبطاقات الهوية، وكاميرات المراقبة، وجمع بيانات الاتّصالات من شركات الاتّصالات، وقواعد البيانات البيومترية. ويركّز حلبي على "المراقبة داخل إسرائيل، وعلى الانتهاك الروتينيّ لأنظمة الحماية من قبل أجهزة المخابرات والشّركة التي تعمل لصالح الأمن القوميّ."⁶

لا يمكن إنكار أثر تكنولوجيا المراقبة الإسرائيليّة على حقوق الإنسان. إذ أثبت أنّ مراقبة الأفراد، والذين عادة ما يكونون من الصحفيين، والنّاشطين، والشّخصيات المعارضة، والنقاد، تؤدّي إلى اعتقالات تعسّفية بحق بعضهم، وتعرّض الأشخاص للتّعذيب، أو القتل خارج نطاق القانون.⁷ كما أنّ الصحفيين ووسائل الإعلام يتعرّضون لمراقبة عسكريّة، وأوامر تحظر تغطية مواضيع معيّنة، ودعاوى قضائيّة من القطاع الخاصّ تهدف إلى تكميم أفواههم.⁸ وقد تسبّب قانونان مهمّان للغاية يرتبطان بالمراقبة الداخليّة لمواطنين إسرائيليين، بإشغال جدل حادّ في الإعلام الإسرائيليّ، ليصل النقاش حولهما إلى المحكمة العليا؛ وهما "قانون الأخ الكبير"، و"قانون قواعد البيانات البيومترية". وقد صادق الكنيست على الأوّل عام 2007، ويسمح هذا القانون للشّركة بإعداد قواعد بيانات للمواطنين، والتي تحتوي على أرقام هواتف (بما يشمل غير المسجّلين)، وأسماء مستخدمي الهواتف المحمولة، والأرقام التسلسليّة للهواتف النّقالة، وخرائط لمواقع الهوائيات. ووصفت قاعدة البيانات هذه بـ"أكبر قاعدة بيانات في الغرب"⁹. وفي 2009، سنّت إسرائيل قانوناً أسّست بموجبه قائمة بيانات بيومترية، تُجمع فيها البيانات البيومترية للمواطنين، وتُخزّن؛ وهذا يشمل البيانات البيولوجيّة المميّزة للأشخاص مثل بصمات الأصابع، وأنماط شبكيّة العين والقزحيّة، والحمض النووي،

⁴ Stevens, Andrew. (2011). Surveillance policies, practices and technologies in Israel and the occupied Palestinian territories: Assessing the security state. The New Transparency Project, Working Paper IV, IRSP IV. Retrieved from: <https://www.sscqueens.org/sites/sscqueens.org/files/2011-11-Stevens-WPIV.pdf>.

⁵Halabi, Usama. (2011). "Legal analysis and critique of some surveillance methods used by Israel.", in E. Zureik, D. Lyon and Y. Abu-Laban (eds). Surveillance and Control in Israel/Palestine: Routledge. Pp. (199-218).

⁶Stevens, Andrew. Ibid. P.2

⁷ United Nations: Human Rights Office of the High Commissioner. (2019). The 2019 report on the surveillance industry. Retrieved from: <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx>

⁸ Reporters without borders. Toxic environment. (2020). Retrieved from: <https://rsf.org/en/israel?nl=ok>

⁹Shahar, Ilan. (2007, 7 December). Big Brother Law' Allows biggest database in West'. HAARETZ. Retrieved in: (2 July 2020), from: <https://www.haaretz.com/1.4967126>



وغيرها من المُعرّفات الخاصّة.¹⁰ كان الدّافع لإنشاء قاعدة البيانات البيومترية، والتي تأخّر إعدادها بعد مشروع تجريبيّ لمُدّة عامين بدأ في آب/ أغسطس 2013، يكمن بالحجّة القائلة بأن هذا النوع من قواعد البيانات، يضمن الأمن والحماية من سرقة المعلومات الشّخصية. عارضت منظمات حقوق الإنسان الحملة البيومترية في إسرائيل، خوفاً من أنّها قد تهدّد الخصوصية الفردية وتمنح الهيئات الحكومية منالية كاملة للبيانات الشّخصية دون تأمين إشراف كافٍ على هذه الممارسات.¹¹

يلفت الباحث الإسرائيليّ المختصّ بالصّناعة الأمنيّة الإسرائيليّة، نيف غوردون، نظرنا إلى حقيقة أنّ صناعة المراقبة الإسرائيليّة تنبع من العلاقات الوثيقة بين الجيش الإسرائيليّ والقطاع التكنولوجيّ الخاصّ. ففي عام 1960 مثلاً، شرع الجيش الإسرائيليّ في تطوير برمجيّة حاسوب قبل تسعة أعوام من إنشاء صناعة البرمجيّات في إسرائيل، وبرامج علم الحاسوب في الجامعات الإسرائيليّة. ويشدّد غوردون أيضاً على أنّ الاحتلال المتواصل المطوّل للضّفة الغربيّة، وقطاع غزّة، والقدس الشّرقية، إلى جانب الحروب الدّورية، يُوقّر لإسرائيل مختبراً واقعياً لاختبار وضبط المنتجات والتّقنيات المختلفة التي تبتكرها.¹² وينتج عن هذه العلاقات الوثيقة بين الجيش والقطاع التكنولوجيّ الإسرائيليّ، حذر تلقائيّ من التّطورات والتّغييرات التكنولوجية، خاصّة لدى الفلسطينيين وناشطي حقوق الإنسان عالمياً. ويشير شيزاف وجاكسون في تقريرهما إلى أنّ "أصبحت إسرائيل مصدرّاً رئيسيّاً لأدوات التّجسس على المدنيّين. يستخدم الدّكاتوريون في جميع أنحاء العالم، وحتى في البلدان التي لا تجمعها علاقات رسميّة بإسرائيل، للتّصنّت على ناشطي حقوق الإنسان، ومراقبة رسائل البريد الإلكترونيّ، واختراق التّطبيقات وتسجيل المحادثات".¹³

في عام 2014، صادقت الحكومة الإسرائيليّة على القرار 1776، ووضعت استراتيجيّة لزيادة مشاريعها الأمنيّة في القدس الشّرقية والقرى والبلدات الفلسطينيّة داخل الخط الأخضر.¹⁴ منذ ذلك الحين، عزّزت الخطّة

¹⁰ Biometrics, as commentators note, establishes a closer link between the biological and political, forging what is known as the biopolitical.

Israel Democracy Institute. (2010). The State of Israel and the Biometric Database Law: Political Centristism and the Post-Democratic State. Retrieved from: <https://en.idi.org.il/articles/6823>

¹¹ Privacy International. (2013, July 22). Israel Launches Controversial Biometric Database. Privacy International, Retrieved from: <https://privacyinternational.org/news-analysis/1181/israel-launches-controversial-biometric-database> ; Jonathan J. Klinger. (2011, June 4). Israel to Start Collecting Fingerprints from All Citizens. +972 Magazine. Retrieved in: (2020, July 5), from: <https://www.972mag.com/israel-to-start-collecting-fingerprints-from-all-citizens/>

¹² Gordon, Neve. (2009, April). The Political Economy of Israel's Homeland Security. The New Transparency Project, Working Paper III. Retrieved from: <https://www.sscqueens.org/sites/sscqueens.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf>

¹³ Shezaf, Hagar; Jacobson, Jonathan. (2018, October 20). Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. HAARETZ. Retrieved in (2020, August 14), from: <https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027>

¹⁴ Prime Minister's Office. (2014, June). Resolution 1775: The Plan to Increase Personal Security and Socio-Economic Development in Jerusalem for the Benefit of All its Residents. Retrieved from: https://www.gov.il/he/departments/prime_ministers_office



ووسّعت. وفي عام 2015، شملت الخطة السنوية للواء شرطة القدس (الإسرائيلية)، تخصيص 48.9 مليون شيكل في تعزيز كاميرات وتقنيات المراقبة في القدس الشرقية، وشراء معدّات جديدة وتركيبها.¹⁵

أنشأت قوانين وآليات المراقبة هذه، منظومة مراقبة شاملة، تنتهك حقّ الفلسطينيين في الخصوصية، وتضاعف التضييق على حرية تعبيرهم، وقدرتهم على المطالبة باحترام حقوق الإنسان خاصّتهم. في غضون ذلك، ومنذ انتشار جائحة فيروس كورونا المستجد، يستخدم جهاز المخابرات الإسرائيلية ("الشاباك")، البيانات حول المواقع الجغرافية للهواتف النقالة الخاصّة بالمواطنين، لتتبع ومراقبة أولئك المصابين بكوفيد-19. ومما يثير الجدل، أنّ هذا النوع من البيانات جُمع أيضًا على مدار الأعوام الماضية دون الإبلاغ عن ذلك مسبقًا.

مع اشتعال نقاش حاد حول استخدام برامج المراقبة الجماعية في إسرائيل، نشر بيرغمان وشايرتوش، مقالًا في غاية الأهمية في موقع "واينت" (Ynet)، في 27 آذار/ مارس 2020،¹⁶ كشف عن معلومات تتعلّق بوجود قاعدة بيانات سرّية تُعرف باسم "الأداة" أو "هكلي" بالعبرية. وأظهر المقال أنّ "الشاباك" يتجسّس على جميع المواطنين باستخدام الاتصالات الإسرائيلية منذ عام 2002، طوال الوقت، والأهمّ من ذلك، أنّ هذا التجسس يتمّ بصرف النظر عن الأزمة الصحيّة الأخيرة، بحيث أنّ كل ما كان على الحكومة الإسرائيلية فعله، هو إتاحة استخدام قاعدة البيانات هذه لمعرفة مكان تواجد المرضى، والأشخاص الذين اختلطوا بهم، وأماكن سفرهم والمزيد.

يكشف تحقيق بيرغمان، أنّ خمسة أعضاء فقط في اللجنة الفرعية للاستخبارات كانوا على علم مسبق بوجود "الأداة"، والتي لم يُلفت انتباه الجمهور الإسرائيليّ إليها من قبل. والنتيجة هي، تفعيل منظومة شاملة لجمع معلومات حول جميع مواطني "دولة ديمقراطية"، ولكنّ سرّية تامّة، ودون شفافية، وبعيدًا عن أعين الجمهور. وفقًا لبيرغمان، فإنّه بالإضافة إلى جمع "الأداة" معلومات عن الجميع، فإنّها تتيح التحقق من حياة أيّ مواطن ليس فقط بالوقت الذي أصبح فيه هدفًا للفحص، بل أيضًا في الفترة السابقة لبدء مراقبته رسميًا. يوضّح جمع بيانات "الشاباك" أنّ المراقبة الحكوميّة الإسرائيليّة لا تقتصر على المواطنين الفلسطينيين. إذ أنّها ممارسة تمسّ حياة المواطن الإسرائيليّ اليهوديّ أيضًا، على الرّغم من أنّها تتخذ أشكالًا مختلفة، وأنّها غير منحصرة باعتباريات ذات نزعة قومية.¹⁷

¹⁵ WhoProfits. (2018, November). "Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem. Retrieved from: <https://whoprofits.org/wp-content/uploads/2018/11/surveil-final.pdf>

¹⁶ Bergman, Ronen; Shbertztuch, Ido. (2020, March 27). The "tool" has been revealed: the secret GSS database that collects your SMS, call and locations. Ynet. Retrieved in (2020, June 29), from: <https://www.ynet.co.il/articles/0,7340,L-5701412,00.html>

¹⁷ Zureik, Elia. (2016). Strategies of surveillance: the Israeli gaze. *Jerusalem Quarterly*, 66, Pp.12-38.



2. تبرير المراقبة الشاملة في إسرائيل خلال تفشي فيروس كورونا

تثير الأزمات العالمية مثل جائحة فيروس كورونا الحالية، خوفًا كبيرًا بين الناس، والذي يكون عادة بمثابة فرصة للدول والحكومات لتبرير سياسات وممارسات تنتهك حقوق المواطنين الأساسية، أو تعتدي عليها، وذلك خلف ستار "توفير الحماية". قد يؤمن السياسيون، وواضعو السياسات، بل وحتى المواطنون العاديون، بشرعية استخدام تقنيات المراقبة إذا ما ساهمت بالحد من انتشار الفيروس، وساعدت بإنقاذ حياة الناس. ووجهة النظر هذه، تسلط الضوء على مسألة جوهرية تتعلق بعواقب تطبيق المراقبة الشاملة، المترتبة على حقوق الإنسان الأساسية، سواء تلك الخاصة بالأفراد أو بالجماعات. وكما يبين التاريخ، فإن "الشاباك" يتدخل في قضايا مدنية، لا سيما تلك المتعلقة بالفلسطينيين الذين يتعرضون للمراقبة والقمع، على المستوى الفردي والسياسي والثقافي.¹⁸ لذا، ينظر الفلسطينيون بعين الريبة للمساعي الرامية إلى توسعة هيكل مراقبة السكان باسم "الكفاءة"، وخاصة التوسعة التي تتمتع بالقدرة على تتبع حركتهم بمنهجية أكبر، وتخزين معلومات شخصية عنهم بشكل فوري. وعليه، فإنه ليس من المفاجئ أن "عدالة - المركز القانوني لحماية حقوق الأقلية العربية في إسرائيل" بالتعاون مع "القائمة المشتركة"، أي التحالف الذي يجمع الأحزاب العربية الكبرى في الكنيست، بادرا لالتماس ضد توسيع صلاحيات "الشاباك".

من أجل الحصول على شرعية جماهيرية لتطبيق أساليب المراقبة الجديدة وتوسيع سلطة "الشاباك"، كانت هناك حاجة لاعتبار أزمة تفشي فيروس كورونا المستجد، خطرًا أمنيًا. ففي إسرائيل، تلعب سياسات التهريب منذ عقود، سواء أكان الخطر حقيقيًا أم متخيلاً، دورًا ناجعًا كاستراتيجية لخلق وحدة قومية قوية، وقمع حقوق الإنسان، وإسكات المعارضة والنقد الداخلي. ويشير الكاتب الإسرائيلي سيث فريدمان، إلى أن دولة إسرائيل تستخدم تاريخ معاناة اليهود اعتبارًا لخلق "ثقافة خوف"¹⁹ سائدة لكي تشرعن إجراءاتها الأمنية الوحشية ضد الفلسطينيين باسم الأمن القومي. وذلك يشمل إنكار حقوق الإنسان الأساسية الخاصة بالفلسطينيين، ومحاولات طمس الرواية الفلسطينية.

2.1 أمنة معالجة فيروس كورونا والحقوق الرقمية في إسرائيل

¹⁸ 7amleh- Arab center for Social Media Advancement. (2020, July). Online Smear Campaigns and Deplatforming: The Silencing and Delegitimization of Palestinian Human Rights Defenders, Activists and Organizations. Retrieved from: <https://7amleh.org/2020/07/02/online-smear-campaigns-and-deplatforming-the-silencing-and-delegitimization-of-palestinian-human-rights-defenders-activists-and-organizations>

¹⁹ Freedman, Seth. (2008, June 22). Culture of Fear. The Guardian. Retrieved in (2020, June 29), from: <https://www.theguardian.com/commentisfree/2008/jun/22/israelandthepalestinians.fear>



بالإضافة إلى تنفيذها إجراءات خاصة بالصحة العامة كالحجر الصحي، والفحوصات، وعمليات الإغلاق، اختارت إسرائيل أيضًا، أن تعتبر فيروس كورونا المستجد خطرًا آمنًا، وليس مجرد أزمة في الصحة العامة.²⁰ في حين يرى الباحثون المختصون في "نظرية الأمانة"، أن الأمانة هي عبارة عن فعل خطائي، الأمر الذي يدفعهم للتركيز على الجوانب البلاغية في تحديد مسائل الأمن القومي، فإن إيهود عيران²¹، يشدد على أن أمانة إسرائيل لفيروس كورونا المستجد، انعكست أيضًا في الخطوات التي اتخذتها الحكومة الإسرائيلية. فبحسب رئيس الحكومة الإسرائيلية، بنيامين نتنياهو، إن الواقع الجديد الذي يتسم بمحاولة السيطرة على تفشي الفيروس، يبرر استخدام إجراءات استثنائية. وصرح نتنياهو أنه ضمن مساعي إسرائيل لمقارعة الوباء، فإن الحكومة ستستخدم ضده "إجراءات لم نستخدمها من قبل إلا ضد الإرهابيين".²² وشملت هذه الإجراءات، استخدامًا استثنائيًا لأجهزة إسرائيل الاستخباراتية المتعددة. فبالإضافة إلى استخدام "الشباك" تقنيات مراقبة لتتبع المواطنين المصابين بفيروس كورونا،²³ استنفرت الفرق الاستخباراتية في الجيش الإسرائيلي، بما في ذلك "قسم الأبحاث" خاصته، ووحدة النخبة "8200" أيضًا، من أجل مساعدة وزارة الصحة في جمع المعلومات الاستخباراتية المرتبطة بفيروس كورونا وتحليلها.²⁴ وأخيرًا، كلف نتنياهو "الموساد"، أي جهاز الاستخبارات الإسرائيلي الخارجي، بـ "فعل كل شيء وأي شيء" لتحصيل أجهزة التنفس الاصطناعي، وغيرها من الإمدادات الطبية من الخارج، ومنحها لوزارة الصحة الإسرائيلية.²⁵ وتعكس هذه الخطوات الطريق الأممي الذي اتخذه إسرائيل في معالجة الجائحة العالمية، باستخدام وحدات عسكرية، وأجهزة استخبارات، وتقنيات، وجمع معلومات استخباراتية لاحتياجات الأمن القومي للبلاد. بعيدًا عن التمعن بأنماط أو أنواع التماذج الفعالة أو غير المجدية في المعركة ضد فيروس كورونا، فإن إجراءات المراقبة

²⁰ Hoffman, Adam. (2020, April). The Securitization of the Coronavirus Crisis in the Middle East. POMEPS Studies (39). Pp: 10-14

https://pomeps.org/wp-content/uploads/2020/04/POMEPS_Studies_39_Web.pdf

²¹ Eiran, Ehud. (2020, April). Israel: Politics and Identity in Coronavirus times. POMEPS Studies (39). Pp: 44-47

https://pomeps.org/wp-content/uploads/2020/04/POMEPS_Studies_39_Web.pdf

²² Sindel, Yonatan. (2020, March 14). Israel: Unveiling broad coronavirus measures, Netanyahu says all leisure activities to be halted. i24NEWS. Retrieved in (2020, June 21),

from: <https://www.i24news.tv/en/news/israel/1584216067-coronavirus-all-leisure-activities-to-be-halted-in-israel-netanyahu-says-unveiling-broad-measures>

²³ Bob, Yonah; Hoffman, Gil. (2020, March 17). Shin Bet confirms it is currently using surveillance tools. THE JERUSALEM POST. Retrieved in (2020, June 24), from:

<https://www.jpost.com/breaking-news/use-of-digital-means-to-track-coronavirus-patients-approved-621237>

²⁴ Zeitun, Yoav. (2020, April 1). Corona's Shadow War in Corona: Collection, Investigator and Decoder. Ynet. Retrieved in (2020, June 24), from: <https://www.ynet.co.il/articles/0,7340,L-5704617,00.html>

²⁵ Caspit, Ben. (2020, April 1). Mossad, Netanyahu's secret weapon against the coronavirus. AL-Monitor. Retrieved in (2020, June 24), from: <https://www.al-monitor.com/pulse/originals/2020/03/israel-benjamin-netanyahu-mossad-coronavirus-test-kits.html>



التي تفرضها إسرائيل في هذه المعركة، يجب أن تدفعنا للتساؤل عن الغرض من وراء التتبع واسع النطاق وطويل الأمد.

2.2 الإطار القانوني لاستخدام برامج المراقبة: توسيع صلاحيات "الشاباك"

تعرف المادة السابعة²⁶ من قانون جهاز الأمن العام، مهمة "الشاباك" على النحو التالي: "حماية أمن الدولة ونظام ومؤسسات النظام الديمقراطي من مخاطر الإرهاب، والتخريب، والتدمير، والتجسس، وإفشاء أسرار الدولة، وعلى الجهاز أن يعمل على حماية وتعزيز مصالح الدولة الأخرى الحيوية للأمن القومي للدولة، كل ذلك على نحو تحدده الحكومة وخاضع لكل قانون". يفسر "الشاباك" هذه المادة بشكل فضفاض، ومن خلال هذا التفسير، يتدخل "الشاباك" في مجالات الحياة المدنية (خاصة حياة الفلسطينيين) باستخدام برامج مراقبة جماعية ضد الفلسطينيين مواطني إسرائيل، والفلسطينيين سكان القدس الشرقية، وأولئك الذين يعيشون في المناطق الفلسطينية المحتلة. أثار توسع صلاحيات "الشاباك" في فترة انتشار فيروس كورونا، جدلاً حاداً، وليس لاستخدام هذه التقنيات، بل بسبب الإقرار باستخدام هذه الأساليب على المواطنين اليهود أيضاً. في 26 نيسان/ أبريل 2020، أصدرت المحكمة العليا الإسرائيلية، قراراً بشأن أربعة التماسات تطعن بقانونية تتبع "الشاباك" ومراقبته للمرضى المصابين بفيروس كورونا المستجد، والأشخاص الذين احتكوا بهم، إماماً من خلال هواتفهم النقالة أو عبر أي وسيلة أخرى.²⁷ بقبول الحجة التي طرحها "عدالة" - المركز القانوني لحماية حقوق الأقلية العربية في إسرائيل"، والتي ادعى من خلالها أن الحكومة تجاوزت سلطتها عند توسيعها نطاق أنشطة "الشاباك" بما يتخطى قضايا الأمن القومي الصارمة، قضت المحكمة العليا بعدم قانونية تتبع "الشاباك" للمواطنين دون مرجع تشريعي، حتى وإن كان ذلك خلال أزمة غير عادية مثل جائحة فيروس كورونا المستجد. ومع ذلك، على الرغم من موقف المحكمة وإقرارها بعدم قانونية المراقبة، إلا أن المحكمة سمحت لـ "الشاباك" بمواصلة برنامج التتبع خاصته، طالما أن الحكومة قد أطلقت عملية تشريعية في الكنيست حتى 30 نيسان/ أبريل 2020.²⁸ بكلمات أخرى، قبلت المحكمة العليا، أن يستمر "الشاباك" في ظروف معينة، بامتلاك سلطة التدخل في قضايا مدنية بما يشمل تلك المتعلقة بالصحة

²⁶ The General Security Service (GSS) Law 5762-2002
https://knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf

²⁷ H CJ 2109/20, Adv. Shahr Ben Meir v. Knesset (joined with H CJ 2135/20, ACRI v. Prime Minister, H CJ 2141/20, Adalah and the Joint List v. The Prime Minister, et. al and H CJ 2187/20, The Journalists' Union in Israel v. Prime Minister) (decision delivered 26 April 2020) available in Hebrew at:
https://www.adalah.org/uploads/uploads/SCT_decision_Shabak_26042020.pdf

²⁸ On 30 April 2020 the Knesset Foreign Affairs and Defense Committee's Subcommittee for Intelligence and Secret Services voted to approve a governmental decision authorizing the Shin Bet to continue the program for another week. Adalah- the Legal center for Arab Minority Rights in Israel sent a letter to the Knesset Committee Chairman, the AG and others on the same day protesting that the government's extension of the program and the subcommittee's approval of it directly contradicts the 26 April Supreme Court ruling. Adalah- the Legal center for Arab Minority Rights in Israel. (2020, May 4). Adalah's Case List: Coronavirus and Human Rights Petitions pending before the Israeli Supreme Court – as of 4 May 2020. Retrieved from:
https://www.adalah.org/uploads/uploads/Adalah_Corona_Petitions_04.05.2020_FINAL.pdf



العامّة، وفقاً لتفسير أنشطته بموجب المادّة السّابعة (بي) (296). (إضافة إلى ذلك، على الرّغم من إدراك المحكمة أنّ برنامج المراقبة الخاصّ بـ "الشّاباك" ينتهك حقوق المواطنين الدّستوريّة، إلّا أنّها لم تمنع الحكومة تماماً من توسعة تدخّل "الشّاباك" في التّعامل مع الأمور المدنيّة. بدلاً من ذلك، أمرت الحكومة وشجّعته على أن تؤسّس عمليّة تشريعيّة يصادق عليها الكنيست، لإنشاء مسار قانونيّ لاستخدام هذا البرنامج. نتيجة لذلك، سيحصل "الشّاباك" على حقّ قانونيّ لمراقبة مواطني إسرائيل.

2.3 أساليب المراقبة الاسرائيلية الشّاملة خلال تفشّي فيروس كورونا

تخترط العديد من السّلطات الإسرائيليّة في تتبّع حركة النّاس، بدءاً من وزارة الصّحة وحتىّ جهاز المخابرات الدّاخليّ المتين، "الشّاباك". وتنطوي أساليب التّتبّع على شبكات مراقبة واسعة، وتحليل وإحالة مرجعيّة لقواعد البيانات الضّخمة، ومراقبة المواقع الجغرافيّة للمواطنين من خلال هواتفهم المحمولة، واستخدام التّعرف على الوجوه على أساس الذّكاء الاصطناعيّ.

- تحديد الموقع الجغرافيّ: فعّل "الشّاباك" تقنيّة لتتبّع المواقع الجغرافيّة للهواتف الذّكيّة للتّجسس على الإسرائيليّين الذين شُخصوا بفيروس كورونا، وتتبع مواقع تواجدهم. تسلّم وزارة الصّحة تفاصيل المرضى الذين ثبتت إصابتهم بفيروس كورونا، لجهاز "الشّاباك"، ويقدم الأخير لها قائمة بتفاصيل جميع الأشخاص الذين اختلط بهم هؤلاء خلال فترة أسبوعين. وأمّا "الاختلاط" بالمريض، فيعرّف على أنّه قضاء ما لا يقل عن 15 دقيقة على مقربة مترين من شخص مصاب بالفيروس. ومن ثمّ يتلقّى الأشخاص الذين وردت أسماءهم على القائمة، رسالة نصيّة تطالبهم بعزل أنفسهم، ممّا يعني أنّ عليهم أن يمشوا في منازلهم، ولا يُسمح لهم بمغادرتها تحت أي ظرف كان. وقضت المحكمة العليا الإسرائيليّة بالسّماح للبرنامج بالاستمرار طالما تشرف عليه لجنة برلمانيّة.
- "هماغين" 30 - "الحامي": بعد مرور ستّة أيام فقط على إطلاق المراقبة الإلزاميّة من "الشّاباك"، أطلقت وزارة الصّحة الإسرائيليّة خدمة تطوعيّة شبيهة للغاية لآليّة عمل برنامج "الشّاباك"، على شكل تطبيق رقميّ مفتوح المصدر، والذي يتيح للمواطنين أن يختاروا تسجيل المواقع الجغرافيّة لتواجد هواتفهم النّقالة. ويقارن هذا التّطبيق سجلّ نظام تحديد المواقع الخاصّ بهاتفك النّقال ("جي بي إس")، مع سجلّ وزارة الصّحة لبيانات أماكن التّواجد الجغرافيّ للمرضى. ويحدّر التّطبيق مستخدمي الهواتف النّقالة بعد فترة وجيزة من احتكاكهم بشخص ثبتت إصابته بفيروس سارس-كوف-2، وينصحهم بالحجر الدّائيّ. أصبح "هماغين"، الكلمة الأكثر بحثاً في إسرائيل على محرّك

²⁹ Ibid

³⁰ Ministry of Health. (2020). HaMagen 2: the National app for fighting the spread of coronavirus. Retrieved from: <https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/>



بحث "جوجل" (Google)، بين ليلة وضحاها. وفي غضون أسبوع، قام أكثر من مليون شخص (أي ما يعادل خمس المستخدمين البالغين للهواتف الذكية في إسرائيل) بتنزيل التطبيق، على الرغم من أنّ البرنامج المشابه، لكن الإلزامي، الذي يديره "الشاباك" كان موجودًا بالفعل.

ومما يثير الاهتمام، أنّ نحو ثلث المستخدمين أزالوا التطبيق عن أجهزتهم بعد وقت قصير من تثبيته عليها، ممّا يعكس نسبة مشاركة كبيرة في التطبيق، ولكنها ليست مثالية.³¹ إنّ إحدى المحدوديات الكبيرة في هذا النهج، هي أنّ مثل هذه التطبيقات لا تساهم بتقليل انتشار المرض إلا إذا استخدمها عدد هائل من الأشخاص. كما ينطوي تسليم البيانات طوعاً، على خطر خلق انطباع خاطئ عن الأمان لدى مستخدمي التطبيق، لأنّ المناطق التي لا توجد بلاغات بشأنها يُمكنها أيضاً أن تكون موبوءة بأشخاص يمكنهم نشر الفيروس. ومع ذلك، قضت المحكمة العليا، عند الاختيار بين برنامج التتبع التابع لـ "الشاباك" والتطبيق الطوعي الخاص بوزارة الصحة، بالسّماح لـ "الشاباك" بالاستمرار في جمع البيانات، بشرط أن يكون هناك أساس تشريعي دائم.

في الطريقتين المُدرجتين أعلاه، فإنّه بسبب صعوبة تحديد مدى التقارب بين الهواتف النقالة، والأهم من ذلك، صعوبة تمييز وجود حواجز مادية كالجدران والأبواب بين المستخدمين، والتي قد تمنع تفشي الفيروس، يمكن أن يؤدي ذلك إلى ارتفاع زائف بمعدلات الإصابات الموجبة.³²

● التعرّف على الوجوه: يُعدّ التعرّف على الوجوه برنامجاً بيومترياً يملك قدرة على تحديد أو التعرّف على شخص، عبر مقارنة وتحليل أنماط تعتمد على ملامح وجهه. وتُستخدم هذه التقنيات في الغالب لأغراض أمنية، ولو أنّ هناك اهتماماً متزايداً في استخدامها في مجالات أخرى. غالباً ما يُستخدم التعرّف على الوجوه كأداة حكومية للمراقبة الشاملة. ويُستخدم أسلوب المراقبة هذا بكثافة عالية في الضفة الغربية المحتلة. بينما تمثّل البلدة القديمة في القدس، نموذجاً مصغراً، حيث تسعى إسرائيل إلى خلق بيئة قهرية تهدف إلى دفع الفلسطينيين أبناء المدينة إلى مغادرتها. ولهذه الغاية، أطلقت إسرائيل مشروع "مبات 2000" في البلدة القديمة، وهو عبارة عن منظومة دائرة مغلقة تجمع ما بين 320 و400 كاميرا مراقبة، بحيث كلّ واحدة منها قادرة على الالتفاف 360 درجة، من أجل تتبّع حركة النّاس ومتابعتها.³³

³¹ Amit, M., Kimhi, H., Bader, T. *et al.* (2020, May 26). Mass-surveillance technologies to fight coronavirus spread: the case of Israel. *Nature medicine*. Retrieved in (2020, June 25), from: <https://www.nature.com/articles/s41591-020-0927-z>

³² Ibid

³³ 7amleh- the Arab center for the Advancement of Social Media. (2020, May 21). Facial Recognition Technology and Palestinian Digital Rights. Retrieved from: <https://7amleh.org/2020/05/21/facial-recognition-technology-and-palestinian-digital-rights>



- كاميرات "عين الصقر"، واسمها بالعبرية "عين هنتس": وهي كاميرات ذكية ترصد لوحات ترخيص المركبات، وتقارن أرقامها مع بيانات محددة مسبقاً في قواعد البيانات، كبيانات المركبات التي أُبلغ عن سرقتها وقاعدة بيانات السيارات التي انتهت مدد صلاحية ترخيصها، وتتبع أصحابها على الفور. نُصب هذا النوع من الكاميرات في كل أنحاء إسرائيل، وهي تجمع معلومات عن حركة المواطنين منذ بدأ عملها في 2013.³⁴ تحتفظ الشرطة الإسرائيلية بقاعدة بيانات حول حركة جميع المواطنين حتى أولئك الذين لم يرتكبوا أي جنحة، والذين لم يكونوا موضع شبهة قط أيضاً، تحسباً من ضلوع مركباتهم بأي جنحة في المستقبل. وبكلمات أخرى، تحتفظ الشرطة بقاعدة بيانات سرية عن حركة المواطنين، والتي قد تبقى بحوزتها لأعوام طويلة. وترفض الشرطة تقديم بيانات حول طرق نشر هذه الكاميرات، أو عددها، أو كمية لوحات ترخيص المركبات التي صورتها، ولا حتى الزمن المحدد الذي حُرّنت فيه هذه البيانات. لم يُبلغ عن قاعدة بيانات "عين هنتس" على النحو المطلوب في مسجل قواعد البيانات في وزارة القضاء الإسرائيلية، واليوم، لا يوجد أي إجراء للشرطة ينظم استخدامها.
- تطبيق "المنسق (COGAT)" تنصح إسرائيل الفلسطينيين الذين يعيشون في المناطق الفلسطينية المحتلة، والذين يحتاجون إلى التأكد إذا ما كانت تصاريحهم لدخول إسرائيل والبقاء فيها لفترات محددة، لا تزال سارية المفعول، أن يثبتوا على أجهزتهم الذكية تطبيقاً يتيح للجيش الإسرائيلي الدخول إليها. والتطبيق الذي يُعرف باسم "المنسق" يسمح لجيش الاحتلال بتتبع موقع جهاز المستخدم الجغرافي، بالإضافة إلى أنه يمنحه منالية للإشعارات التي يتلقاها المستخدم، والملفات التي ينزلها أو يحفظها، والكاميرا الخاصة بالجهاز. نتيجة لتفشي فيروس كورونا المستجد، أغلق "مكتب الارتباط" جميع مكاتبه. ومن أجل تثبيت التطبيق على أجهزة المستخدمين، فإنه يضطرون إلى المصادقة على الشروط التالية: "يجوز لنا استخدام المعلومات التي نجمعها لأي غرض كان، بما في ذلك الأغراض الأمنية".³⁵ إضافة إلى الانتهاك المباشر للحقوق الرقمية للفلسطينيين الذين يعيشون في الأراضي المحتلة، فإن المواطنين في إسرائيل الذين على اتصال مباشر معهم، يصبحون عرضة لهذه المخاطر أيضاً.

استنتاجات وتوصيات

يتعرض جميع مواطني إسرائيل لانتهاكات لحقوقهم الرقمية. ومع ذلك، فإن الفلسطينيين مواطني إسرائيل، شأنهم شأن أبناء شعبهم في الأراضي المحتلة، هم الفئة الأقل حصانة أمام هذه الانتهاكات، سواء عبر الإنترنت

³⁴ Dolev, Daniel. (2020, May 6). Walla! NEWS: Police hold a confidential database on civilian movements. Walla. Retrieved in (2020, July 25), from: <https://news.walla.co.il/item/3355178>

³⁵ Middle East Eye. (2020). 'The Coordinator': Israel instructs Palestinians to download app that tracks their phones. Retrieved from: <https://www.middleeasteye.net/news/coordinator-israel-instructs-palestinians-download-app-tracks-their-phones>

أم خارجه. أدى تأطير جائحة فيروس كورونا تحت خانة التهديد الأمني، إلى إضفاء شرعية على استخدام أساليب المراقبة الجماعية وتوسيع نطاق صلاحيات "الشبابك"، مما يجعل الفلسطينيين أكثر عرضة للانتهاكات، إلى جانب جماعات أخرى كناشطي حقوق الإنسان والمدافعين عنها، والمنظمات والصحافيين الذين ينتقدون الحكومة الإسرائيلية.

علاوة على المخاوف بشأن الخصوصية والمساءلة، يشعر النقاد بقلق من التدايعات طويلة الأمد لممارسات "الشبابك" خلال هذه الأزمة، ومن التطبيع مع استخدام أساليب المراقبة الجماعية. أعرب "عدالة - المركز القانوني لحماية حقوق الأقلية العربية في إسرائيل"، عن قلقه من ترك المحكمة العليا الباب مفتوح أمام مزيد من تدخل "الشبابك" في الشؤون المدنية. لأول مرة، ينجح المستوى السياسي، بالحصول على موافقة الكنيست، لتحويل عمل "الشبابك" وأحد أهم أدواته، لصالح أمر آخر لا علاقة له بالمسائل الأمنية.

وبهذا المعنى، فإنّ جائحة فيروس كورونا تخدم غطاءً مثاليًا لـ "الشبابك"، لإضفاء شرعية على استخدامه لبرامج المراقبة الجماعية، والإعلان عن ذلك. ومن شأن ذلك أن يفسر ردود أفعال كبار مسؤولي "الشبابك"، عندما عبّروا عن ذهولهم بالمؤتمرات الصحافية التي تحدّث خلالها نتيهاهو للعالم كلّه عن قدرات "الشبابك".

وفي حين أنّ هذا التطور نحو الاستخدام الشرعي والعلني لتقنيات المراقبة، مُقلق بشكل خاصّ بالنسبة للفلسطينيين، فإنّه بالإمكان فهمه أيضًا، كخطوة خطيرة بسبب قدرة المساهمة التي تملكها، في التضييق الأوسع لمساحة عمل منظمات المجتمع المدني، والإسكات المستمر للمدافعين عن حقوق الإنسان، وناشطيها حول العالم. وادّعت منظمة العفو الدولية في تقريرها الأول³⁶ حول استخدام برامج التجسس التي ابتكرتها مجموعة "إن إس أو" الإسرائيلية، ضدّ المدافعين عن حقوق الإنسان في المغرب، أنّ فاعلين حكوميين من أنحاء مختلفة من العالم، استخدموا برمجية اختراق الهواتف سيئة السمعة التي طوّرتها "إن إس أو" باسم "بيغاسوس"، للتجسس على صحافيين وناشطين، ولا سيّما التجسس على أعضاء منظمة العفو الدولية.³⁷ يؤكّد التطبيع مع استخدام تقنيات المراقبة الجماعية على الجوانب الاستبدادية أينما استُخدمت التكنولوجيا لفرض إرادة الدولة، والسيطرة على سلوك المواطنين.

أخيرًا، من أجل حماية الحقوق الرقمية، من الضروريّ ضمان مساحة رقمية مجانية وآمنة ومتساوية للجميع، ولا سيّما للمجموعات الاجتماعية والوطنية والسياسية. وبهذا المعنى، يُعدّ الفلسطينيون الأكثر تضررًا وتعرّضًا لسياسات الرقابة الإسرائيلية. ينبغي اتخاذ خطوات قليلة في الاعتبار. أولًا، مراقبة تقنيات المراقبة الجماعية كجزء من النشاط الرقمي الواسع وحركة المقاومة. من الضروريّ تحديد موقع التجربة الفلسطينية

³⁶ Amnesty International. (2019, October). Morocco: Human Rights Defenders Targeted with NSO Group's Spyware. Retrieved from: <https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/>

³⁷ Amnesty International. (2020, June 22). Moroccan Journalist Targeted with Injection Attacks Using NSO Group's Tools. Retrieved from: <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>



ضمن الجهود الدوليّة لحماية الحقوق الرقمية والحريّات المدنيّة. يمكن القيام بذلك من خلال الإجراءات المستمرة للبحث عن، وتتبع انتهاكات الحقوق الرقمية الفلسطينيّة. ثانيًا، من الصّورويّ الكشف عن هياكل السّلطة المخفيّة في إسرائيل، والتي يتم تغليفها بمجموعة من القوانين والتشريعات المكتوبة مثل سلطات "الشّباك". حتى الآن، عندما ينتهي الوباء، من الصّورويّ أن تتابع عن كثب تقنيّات المراقبة غير العادية هذه.

- د. نجمة علي باحثة ومحللة سياسات ، حاصلة على درجة الدكتوراه من جامعة أوتاغو في نيوزيلندا. يركز بحثها على المقاومة والنشاط داخل الجماعات المضطهدة ، وخاصة بين النشطاء الفلسطينيين في إسرائيل. تكتب نجمة بانتظام في الشبكة: شبكة السياسة الفلسطينية ، وتقدم الاستشارات السياسية حول سياسات الشرق الأوسط ، وبشكل أساسي حول الصراع الإسرائيلي الفلسطيني.