

Israeli Impact on Palestinian Digital Rights During the Coronavirus Pandemic

by Dr. Nijmeh Ali *

In response to the coronavirus pandemic, states are increasingly using dangerous technologies at the cost of protecting fundamental human rights. In March 2020, the Israeli government approved two emergency regulations¹ that served two purposes, first; enforcing new social isolation rules, and secondly; tracking the locations of patients infected with the virus. The mission was allocated to Israel's domestic security agency, the Shin Bet (also known as the General Security Service (GSS) or the Shabak). Privacy and human rights activists have responded with outrage as this is an expansion of the Israeli government's use of mass surveillance technologies, especially by Shin Bet, and is a further violation of digital rights and human rights.

The purpose of this report is to document the deployment of mass surveillance technologies by Israel during the coronavirus pandemic and explore the impact of these policies and practices on Palestinian digital rights -- the right to privacy, freedom of expression and data protection. It also exposes the securitization framework, how the coronavirus has created an opportunity for states to frame policies and practices as necessary for security, leading to expansion and a sense of normalization with mass surveillance in the time of crises.

This report is based on media articles, academic journals and books, as well as position papers and statements from civil society organizations. It begins by looking at the construction of the online surveillance regime in Israel and then focuses on state surveillance during the coronavirus time; presenting online surveillance laws adopted by the Israeli government and its implications on digital rights. The third sections specified mass surveillance technologies used to tackle the coronavirus and highlights the negative impact on the right to privacy and data protection that these technologies can have on all individuals in Israel and the Palestinian occupied territories, including Israeli Jews, as well as how these technologies are used to target specific groups of the population systematically. The adoption of mass surveillance strategies also raises issues of discriminatory policies exposing the 'technological face' of Israeli oppression. Finally, to protect digital rights

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/>

in Israel and Palestinian occupied territories, the paper offers recommendations for ensuring a free, safe and equal digital space for everyone - particularly for social, national and political groups such as Palestinian citizens in Israel and Palestinians of the occupied territories.

1. Constructing the Israeli online surveillance regime

Online surveillance or the surveillance of communication networks, is an intelligence activity designed to gather, retain, process, and analyze digital information from electronic communication networks - landline , cellular networks, the internet or data networks. Surveillance starts by intercepting and retrieving information from the web, collection of communication data, and communications service providers or companies, and processing open and hidden information which can include data- mining techniques.²

In a time in which, massive human communication is conducted via electronic media, controlling modern technology for comprehensive-scale collection, storage and statistical analysis of data can yield more productive and more detailed intelligence information on surveillance targets than ever before. However, this is a double-edged sword when it comes to human rights and the violation of privacy and data protection, taking into consideration that Not only those whom under surveillance are targeted, but also those with whom they are in contact. The additional element is related to the harm caused to individuals by online surveillance- is not limited to their right to privacy. More broadly, the effect produced by such monitoring may harm their general sense of freedom and their freedom of expression.³ When individuals are aware that they are or may be under surveillance, they are likely to modify their behaviour accordingly and enhance their internal sense of censorship. For years, Israel has been using mass surveillance to monitor Palestinians in the occupied Palestinian territories and in Israel, yet, since the outbreak of the Coronavirus, Israel has turned its sophisticated technology to track its Jewish citizens openly. However, the following section reveals that Israel has also been monitoring its citizens away before the Coronavirus.

1.1. Genealogy of online surveillance laws in Israel and human rights violations

Israel presents itself as a country with various legislation covering privacy laws including Section 7 of the Basic Law on Human Dignity and Freedom; Protection of Privacy Law; Registrar of Databases; Credit Data Service Law; Secret Monitoring Law (1979); the Computer Law (1995); Genetic Information Law; and Freedom of Information Law. Based on this, the European Commission considers Israel's data protection laws sufficient for providing a

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

level of protection for personal data transferred from countries in the EU.⁴ A critical view of Israel's security legislation is offered by Halabi⁵ who provides a detailed review of surveillance technologies and practices - ID cards, CCTV, the gathering of communication data from communication companies, and biometric databases - installed by Israel on Israeli citizens. Halabi focuses on "surveillance within Israel, and the routine violation of these protections by state intelligence and police agencies working in the interest of national security."⁶

The impact of Israeli surveillance technology on human rights is undeniable. Surveillance of individuals - often journalists, activists, opposition figures and critics - has been shown to lead to arbitrary detention, torture, and extrajudicial killings.⁷ Journalists and media have also been subjected to military censorship, orders banning coverage of specific subjects and private-sector lawsuits designed to gag them.⁸ In particular, two significant laws related to internal surveillance on Israeli citizens caused a heated debate in the Israeli media and reached the Court; 'The Big Brother Law', and 'The Biometric Database Law'. The Big Brother Law approved by the Knesset in 2007 allows the police to set up a database on citizens that contains telephone numbers (including unlisted ones), names of mobile telephone subscribers, serial numbers of mobile phones, and maps of antenna locations. The database has been described as the "biggest database in the West."⁹ In 2009, Israel passed a law that would establish a biometric database, collecting and storing biometric data - that is, distinguishing biological traits such as fingerprints, retina and iris patterns, DNA, and other unique identifiers.¹⁰ The motivation behind the biometric database, whose implementation was delayed following a two-year pilot project that started in August 2013, is the argument that it ensures security and protection against

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>.

5 Halabi, 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).

6 Stevens, 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>

9 Shahar, 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>

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 Centrism and the Post-Democratic State. Retrieved from:

<https://en.idi.org.il/articles/6823>

theft of personal information. Human rights organizations opposed the biometric campaign in Israel for fear that it would compromise individual privacy and give governmental bodies full access to personal data without securing sufficient oversight.¹¹

Neve Gordon, an Israeli scholar who studied the Israeli security industry, draws our attention to the fact that Israel's surveillance industry stems from the close links between the Israel's military and the technology sector. In 1960, the Israeli military was developing computer software — nine years before the Israeli software industry and university computer science programs even existed. Gordon also emphasizes that the prolonged occupation of the West Bank, Gaza, and East Jerusalem, along with its periodic wars, provides a laboratory for testing and fine-tuning different products that are created or different technologies.¹² These links create an automatic suspect attitude towards technological changes, mainly among Palestinians and human right activists worldwide. "Israel has become a leading exporter of tools for spying on civilians. Dictators around the world – even in countries with no formal ties to Israel – use them to eavesdrop on human rights activists, monitor emails, hack into apps and record conversations".¹³

In 2014, the Israeli government approved Resolution 1775 and put forward a strategy for increasing security in East Jerusalem and Palestinian communities within the Green Line (Israel).¹⁴ Since then, the plan has been reinforced and expanded. In 2015, the Jerusalem Police district plan included the investment of 48.9 million NIS in the strengthening, purchase and installation of CCTV cameras and surveillance technology in East Jerusalem.¹⁵ These laws and surveillance methods established a comprehensive monitoring system, violating Palestinians' right to privacy, and further

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

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>

limiting their right to freedom of expression and their ability to demand their human rights be respected. Meanwhile, during the coronavirus pandemic, Israel's security agency; the Shin Bet, is using citizens' cell phone location data to track and monitor the movements of those infected. Controversially, the data has been collected over the past few years without being previously reported.

With the outbreak of the discussion on using mass surveillance programs in Israel, Bergman and Shabertoch, reviled a vital piece published in Ynet on 27 March 2020,¹⁶ disclosing information regarding a secret database known as the 'tool' or 'Ha kle' in Hebrew. This revealed that the Shin Bet has been spying on all citizens using Israeli telecommunications since 2002, all the time, and most importantly regardless of the health crisis. All that the Israeli government had to do was allow the use of this database to know where patients were, who they talked to, where they traveled and more.

Bergman investigation reveals that only five members of the Intelligence Subcommittee knew about the 'tool,' and it was never brought to the attention of the public in Israel. The result is that an extensive system, which collects information about all citizens of a 'democratic state,' remains entirely in the dark, with no transparency and away from the public eyes. According to Bergman, apart from gathering information on everyone, the 'tool' allows checking citizen life not only from the time they became a subject of examination but also back in time. The Shin Bet data collection makes it clear that Israeli state surveillance is not limited to Palestinian citizens; it touches the lives of the Jewish as well, although it takes different forms and is not so bound up with nationalistic considerations.¹⁷

2. Justification of mass surveillance in Israel during the Coronavirus

Global crises such as the current coronavirus pandemic, evoke great fear among people, which is often an opportunity for states to justify policies and practices that violate or abuse citizen's fundamental rights under the guise of protection. Politicians, policymakers and even ordinary citizens in Israel may believe that surveillance technologies are legitimate if they limit the spread of the virus and save lives. Such a perspective raises a fundamental question regarding the consequences of applying mass surveillance, on fundamental human rights of individuals and groups. As history has shown, the Israeli Shin Bet has intervened in civilian matters, particularly regarding Palestinians whose individual, cultural and political lives have been a target

16 Bergman, Ronen; Shbertztuch, Ido. (2020, March 27).The "tool" has been revealed: the secret GSS database that collects your SMS,calla 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.

of surveillance and repression.¹⁸ Palestinians, therefore, carefully considered any efforts to expand structures of population monitoring in the name of efficiency, particularly one that has the potential to track their movements more systematically and store personal information about them in real-time. Therefore, the petition against the expanding of the Shin Bet's powers, initiated by Adalah: the Legal Centre for the Arab minority in Israel and the Joint List: the Political alliance of the main Arab political parties in Israel, is not surprising.¹⁹

To gain public legitimacy, to apply surveillance methods and expand the Shin Bet's authority, there was a need to frame the coronavirus as a security threat. In Israel, whether it is a real or imagined threat, the politics of fear has been an effective strategy for creating strong national unity and suppressing human rights, opposition and internal criticism for decades. Israeli writer Seth Freedman points out that the Jewish history of suffering is used callously by the State of Israel to create a permanent "culture of fear"²⁰ to justify its brutal security measures toward the Palestinians in the name of national security, this includes rejecting Palestinians fundamental human rights and silencing the Palestinian narrative.

2.1 The Securitization of Coronavirus and digital rights in Israel

In addition to implementing public health measures such as quarantines, tests and lockdowns, Israel also chose to frame the Coronavirus as a security threat and not merely as a public health issue²¹. While scholars of securitization theory view securitization as a speech act and therefore focus on the rhetorical aspects of defining matters of national security, Ehud Eiran²², emphasizes that Israel's Securitization of the coronavirus was also

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 Adalah- the Legal center for Arab Minority Rights in Israel. (2020, May). Adalah's initial analysis of the Shin Bet ("Shabak") Coronavirus Cellphone Surveillance Case. Retrieved from:
https://www.adalah.org/uploads/uploads/Adalah_Initial_Analysis_Shin_Bet_Corona_Surveillanc_e_Case_Final_04.05.2020.pdf

20 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>

21 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

22 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

reflected in the actions undertaken by the Israeli government. According to Netanyahu, the new reality of trying to contain the coronavirus justifies the use of extraordinary measures. Netanyahu stated that as part of Israel's efforts to combat the epidemic, the government would "deploy against it measures we have only previously deployed against terrorists."²³ These measures included an extraordinary use of Israel's various security and intelligence agencies. In addition to the Shin Bet use of surveillance technologies to track citizens infected by the Coronavirus,²⁴ The Israeli army Intelligence Corps, including its Research Division and elite Unit 8200, were also called on to assist the Ministry of Health in collecting and analyzing intelligence related to the Coronavirus.²⁵ Finally, Mossad, Israel's foreign intelligence service, was tasked by Netanyahu "to do everything and anything" to procure ventilators and other needed medical supplies from abroad for the country's health system.²⁶ These steps reflect Israel's securitized response to the global epidemic - using military units, intelligence agents and technologies and collecting intelligence for the country's national security needs. Far from serving as a paradigm of what is active and efficient in the war against Coronavirus, the surveillance measures being imposed in Israel should lead us to question the very purpose of large-scale tracking in the long-term.

2.2 The Legal Framework for using surveillance programs: expanding the Shin Bet authorities

Article 7 (a)²⁷ defines the Shin Bet's mission as: "The protection of State security and the order and institutions of the democratic regime against

23 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>

24 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>

25 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>

26 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>

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

threats of terrorism, sabotage, subversion, espionage and disclosure of State secrets, and the Service shall also act to safeguard and promote other State interests vital for national State security, all as prescribed by the Government and subject to every law.” The Shin Bet interprets this provision widely, and through it intervened in domains of civilian life (mainly of Palestinians) using mass surveillance programs on Palestinian citizens of Israel and Palestinian residents of East Jerusalem and those who live in the occupied Palestinian territories. The expansion of the Shin Bet's authorities during the coronavirus pandemic has created an intense controversy, not over employing such techniques, but over the acknowledgement of using these methods also on Jewish citizens. On 26 April 2020, the Israeli Supreme Court issued a decision on four petitions challenging the legality of the Shin Bet's tracking and monitoring of coronavirus patients and people who came within their vicinity, via their cell phones and by other methods.²⁸Accepting the argument initiated by Adalah- the legal center for Arab minority rights in Israel- arguing the government exceeded its power in expanding the scope of the Shin Bet's activities beyond issues of strict national security, the Israeli court ruled that the Shin Bet cannot track citizens without legislative reference, even during the exceptional coronavirus pandemic. However, despite the court's position and acknowledgement of the illegality, the court allowed the Shin Bet's tracking program to continue, as long as the government initiated a legislative process in the Knesset by 30 April 2020.²⁹ In other words, the court accepted that, under certain circumstances, the Shin Bet still has authority to interfere in civilian issues including those of related to public health, as part of the interpretation of its activities under Article 7 (b)(6)³⁰. Also, despite the court's recognition of the Shin Bet's surveillance program as a breach of citizen's constitutional rights, it did not entirely ban or prevent the government from expanding the Shin Bet's interference with handling civilian matters. Instead, it instructed and encouraged the state to establish a legislative process approved by the Knesset, to create a lawful path for using these programs. As a result, the Shin Bet will have the legal right to surveil Israeli citizens.

28 HCJ 2109/20, Adv. Shahr Ben Meir v. Knesset (joined with HCJ 2135/20, ACRI v. Prime Minister, HCJ 2141/20, Adalah and the Joint List v. The Prime Minister, et. al and HCJ 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

29 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

30 Ibid

2.3 Mass surveillance methods in Israel during the Coronavirus

Numerous authorities are involved in tracking people's movements - ranging from the Health Ministry to the robust domestic intelligence services, the Shin Bet. Tracking methods include extensive surveillance networks, analysis and cross-referencing of massive databases, monitoring the location of citizens through their mobile phones, and using face recognition based on artificial intelligence.

- **Geolocation tracking** - The Shin Bet launched mobile phone location tracking technology to spy on and track Israelis diagnosed with the coronavirus. The ministry of Health hands over the details of patients who tested positive to the coronavirus to Shin Bet and Shin Bet gives them back a list of every person they have been in contact with over the past two weeks. Being 'in contact' is defined as spending a minimum of 15 minutes within two meters of the infected person. The people on that list then receive a text message requesting them to go into isolation, meaning they have to stay home and are not allowed to go out under any circumstance. The Israeli Supreme Court ruled that the program is allowed to continue as long a parliamentary committee oversees it.
- **HaMagen³¹- 'The Protector'** - Six days after the initiation of mandatory coronavirus surveillance by the Shin Bet, the Ministry of Health in Israel launched a very similar voluntary service; an open-code application that allows citizens to opt into the logging of their mobile-phone locations. This app cross-checks the GPS history of your mobile phone with historical geographic data of patients from the ministry of health. It notifies mobile users shortly after they come close to a person who has tested positive for SARS-CoV-2 and advises them to self-isolate. HaMagen became the most-searched item on Google in Israel overnight. Within a week, over a million people (nearly 20% of the adult smartphone users in Israel) had downloaded the application, even though the similar non-voluntary service run by the Shin Bet already existed.

Interestingly, nearly one-third of the users removed the application shortly after installing it on their device, reflective of a substantial, yet not perfect, participation rate.³² A considerable limitation of this approach is that such apps can reduce the spread of disease only if many people use them. Also, voluntary data submission carries a risk of creating a false impression of security for users because areas without reports might still have infected

31 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/>

32 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>

people who can spread the virus. However, The Supreme Court ruled, when choosing between the Shin Bet's tracking programme and the Ministry of Health approved voluntary application, to allow the Shin Bet to continue with their data collection, with the condition that there needs to be based on permanent legislation.

In the first two methods, because of the difficulty of determining closeness among phones and, more importantly, the physical barriers such as walls and doors between users that might prevent transmission, this can result in a high false-positive rate.³³

- **Facial recognition:** Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use. Facial recognition is often used as a mass surveillance technique by governments. This surveillance method is heavily used in the West Bank. The Old City of Jerusalem represents a microcosm of this method, where Israel seeks to create a coercive environment aimed at driving Palestinians out of the city. To this end, Israel launched the 'Mabat 2000' project in the Old City, which is a system of 320-400, closed-circuit television (CCTV) cameras capable of manoeuvring 360 degrees to follow and track movements.³⁴
- **The 'Hawk's Eye' cameras, in Hebrew 'Ein H' Nets':** Smart Cameras that detect license plates, compare license numbers to predefined databases, such as the database of vehicles reported as stolen and the database of vehicles whose license has expired, and alert them in real time. These kinds of cameras have been deployed all over Israel and information regarding civilian movement has been collected since 2013.³⁵ The police keep a database of movements of civilians who have not committed any offense, and are not even suspected of it, just in case their vehicle is involved in the offense in the future. In other words, the police hold a confidential database on civilian movement that may remain in the hands of the police for years. The Police refuse to provide data regarding the deployment of the cameras, their number, the amount of license plates captured on them or the exact length of time the data was stored. 'Ein H' Nets'

33 Ibid

34 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>

35 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>

database has not been reported as required to the Registrar of Databases in the Ministry of Justice, and today there is not even a police procedure that regulates its use.

- **COGAT App:** Palestinians living in the Palestinian occupied territories and who need to verify whether their permits to enter and remain in Israel are still valid have been advised by Israel to download an app that enables the military access to their mobile phones. The app, known as 'Al Munasiq,' in Arabic, or 'The Coordinator', allows the army to track the user's phone location as well as access any notifications they receive, files they download or save, and the device's camera. As a result of the Coronavirus outbreak, the Coordination of Government Activities in the Territories (COGAT) offices are now closed. In order to install the app, users need to approve the following terms: "We may make use of the information we collect for any purpose, including for security purposes."³⁶ In addition to the direct damage of digital rights of Palestinians living in the Palestinian territories, Israeli citizens who are in contact with them, are also exposed.

Conclusion and recommendations

All citizens of Israel are experiencing violations of their digital rights. However, Palestinian citizens in Israel, as like Palestinians in the occupied territories, are the most vulnerable group, online and offline. Framing the coronavirus pandemic as a security threat legitimized the use of mass surveillance methods and extended the Shin Bet authorities making Palestinians even more vulnerable alongside with other groups and human rights activists, defenders, organizations, and journalists criticizing the government.

Beyond the concerns over privacy and accountability, critics are also worried about the long-term implications of the Shin Bet's actions during this crisis and the normalization of using mass surveillance methods. Adalah- the legal centre for Arab minority rights in Israel, has expressed concern that the Supreme Court left the door open for the Shin Bet's further involvement in civilian matters. For the first time, a political level, with the approval of the Knesset's unanimous decision, succeeds in diverting the Shin Bet and one of its most essential tools in favour of another matter, which has nothing to do with security issues.

In this sense, the coronavirus pandemic serves as a perfect cover for the Shin Bet to legitimize and declare on using mass surveillance programs. This might explain the reaction of Shin Bet senior officials. They looked on in amazement at the press conferences, during which Netanyahu spoke to the entire world about the Shin Bet capabilities.

36 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>

While this is particularly concerning for Palestinians, it can also be understood as dangerous for the potential it has to contribute more broadly to global shrinking space for civil society organizations and the continued silencing of human rights defenders, activists and organizations worldwide. Amnesty International had claimed in its first report³⁷ on the use of spyware produced by Israeli company NSO group against Moroccan human rights defenders, that governments across the globe have used NSO cell phone hacking software Pegasus to spy on journalists and activists, and in particular spy on a member of Amnesty International.³⁸ Normalizing the use of mass surveillance technologies emphasize authoritarian aspects where technology is used to impose the will of the state, and control citizens behaviour.

Finally, to protect digital rights, it is fundamental to ensure a free, safe and equal digital space for everyone - particularly for social, national and political groups. Palestinians in this sense, are the most harmed and subjected to Israeli policies of surveillance. Few steps should be taken into consideration. First, to monitor mass surveillance technologies as part of broad digital activism and resistance movement. It is essential to locate the Palestinian experience within international efforts of protecting digital rights and civil liberties. This could be done with the continuing actions of researching and tracking violations of Palestinian digital rights. Secondly, it is crucial to uncovering hidden power structures in Israel, which are encapsulated with a set of written rules and regulations such as the Shin Bet authorities. Up to now, when the pandemic is over it is essential to keep close track on such extraordinary surveillance technologies.

***Dr Nijmeh Ali** is a researcher and policy analyst, with a PhD from the University of Otago in New Zealand. Her research focuses on resistance and activism within oppressed groups, particularly among Palestinian activists in Israel. Nijmeh writes regularly in al-shabaka: the Palestinian policy network, and provides political consultancy on Middle Eastern politics, mainly on the Israeli Palestinian conflict.

37 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/>

38 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/>