Arab Reform Initiative

Bawader / Commentary, 11 October 2018

Policing the Digital Sphere: The Impact of Palestine's Cybercrime Legislation

Chiara Ayad

Law 16 refers to Palestine's first Cybercrime Legislation.

This paper lays out fundamental issues about transparency in legislative processes and government accountability in establishing legal frameworks for the protection of citizens in the Palestinian context. It addresses how a protective citizen-centered cyber-security law that seeks to improve citizens' digital security can become a tool for quashing civil dissent and silencing political opposition. Certainly, the Israeli government's practices of mass surveillance and control of ICT infrastructure limit the protective capacity of Palestinian cybersecurity measures. However, this paper will not focus on the role of the Israeli government but rather on the role the Palestinian government has had in increasing its citizens fear of surveillance and insecurity on digital platforms. By examining the Palestinian Authority's first cybercrime legislation, Law no. (16), the paper will discuss how such measures have backlashed, negatively impacting civil liberties and the general political climate. It will also discuss the role civil society organizations had in pressuring the government to issue new cybercrime legislation, law no. (10).

Necessary legislation, secretive enactment

On 24 June 2017, President of the Palestinian Authority, Mahmoud Abbas, passed cybercrime legislation no. (16) by presidential decree. It was passed in secrecy and directly enforced without a period of consultation with civil society organizations. Before the law was issued, Palestinian prosecutors in the West Bank used the 1996 Wireless and Telecommunications law, the 2013 Electronic Transactions law and interpretations of the 1960 Jordanian Penal Code to prosecute crimes committed via computer networks and ICTs. However, this legislation mostly criminalized offenses against physical rather than virtual assets and identity, and loopholes remained in the legal basis for prosecution. Legal experts such as Mustafa Abdelbaqi underlined that the legal framework that existed in Palestine before the issue of the cybercrime law required development in defining cyber offenses and was insufficient to combat the illegal abuse of the internet, data and computer systems.[1] Palestinian police shared this view, stressing that the new law would enable the effective criminalization, prosecution and the collection of evidence on cybercrimes.

Since 2015, electronic crimes have been on the rise in Palestine, both in the Hamas-ruled Gaza Strip and the West Bank. They include identity theft, defamation and most commonly blackmail and sextortion of women. The Palestinian cybercrime unit has launched investigations into cyber crimes committed by and against Palestinian citizens from countries such as Nigeria and Morocco. And Palestinian ministries and officials have been previously targeted by spear-phishing and hacking campaigns. According to the Palestinian police, this rise in cybercrime is attributed to two main factors. The first is increased internet connectivity and use of social media. The second is the absence of laws to allow law enforcement officers to prosecute crimes committed through computer networks.[2]

The Palestinian cybercrime law no. (16) includes 61 provisions that penalize identity theft, fraud and forgery, child pornography as well as other crimes committed through digital means and computer networks.[3] According to Palestinian officials and police, it is a necessary legislation that closes loopholes and allows for the prosecution of cybercrimes. However, because of the secretive manner in which it was passed and its immediate use to prosecute and imprison activists and dissidents, Palestinian civil society organizations campaigned to call for its boycott and reform.

Building on Israeli surveillance policies

Palestinian's online activity has for long been closely monitored by the Israeli authorities, through policies of mass surveillance to identify calls for resistance or violence, as well as information that can be used to entice collaboration with Israeli security forces. The term "isqat" is commonly used among Palestinians when referring to a practice conducted by Israeli intelligence units using information or imagery collected with the aim of blackmailing Palestinians into collaborating with Israeli forces. Former IDF soldiers have spoken out about this practice indicating that the intelligence units unjustifiably violate individual rights and sometimes extort individuals into collaboration.[4] Due to social stigma regarding minority sexual identities, the Palestinian LGBTIQ+ community is a primary target of "isqat".

Further, Palestinians risk being charged with incitement to violence when, for

example, someone documents and shares footage of confrontations with IDF soldiers or poems that call for "resistance". In turn practices of online mass surveillance and harsh criminalization also limit the critique and documentation of occupation policies. Nonetheless, the Israeli attempt at curbing violence remain one-sided as there are very few efforts to address Israeli incitement. A 2018 study by 7amleh, Vigo Social Intelligence and Berl Katznelson Foundation found that every 71 second Israelis publish inciting posts calling for violence against Palestinians. From the controversial Israeli Facebook bill that facilitates the shutdown of Palestinian social media pages to legislation that criminalizes filming Israeli soldiers, the digital sphere is far from being a safe space for Palestinian free expression.[5] With the issue of cybercrime law no. (16), a key concern has been the role it could play in deepening Israeli surveillance considering the PA's widely controversial commitment to security coordination with Israeli security units.

Law no. (16): Civil liberties, privacy and press freedoms under threat

Cybercrime law no. (16) imposes penalties including imprisonment and 2,000 to 10,000 Jordanian dinars (2,820 to 14,000 USD) for crimes of human trafficking, racial discrimination, terrorism financing, drug and narcotic promotion as well as other crimes committed through the Internet and computer technologies. The law equally imposes such penalties on those who digitally produce or share "immoral material" or material that jeopardizes "the public order", allowing for increased social sanctioning and surveillance by security forces. And like other legislation in the region, the 2017 legislation lacks clear definitions of terms such as "public morality", "public order", "national security" and "national unity" that in turn leads to the instrumentalization of such provisions.

In the absence of data protection legislation and necessary safeguards, as well as consultations with civil society organizations working on digital rights, law no. (16) leaves citizen data vulnerable to surveillance by state security apparatuses and threatens privacy rights. Without informing or consulting with Palestinian Internet Service Providers (ISP), the law grants authorities the right to access citizen data under Article 32 which obliges ISP's to provide information, withhold subscriber

data for three years and monitor communications upon the request of the authorities. Such legislation that has been imposed rather than co-developed with ISPs and civil society leaves citizens uninformed of such interventions, thus increasing vulnerability of their communications and data.

Civil society backlash and pressure for amendments

The original cybercrime legislation, law no. (16), also jeopardizes freedom of expression, access to information and particularly press freedoms. In the first month of its entry into force, six Palestinian journalists were arrested by the Palestinian intelligence forces using Article 20. They were suspected of collaboration with unidentified hostile entities; most of the journalists worked for outlets affiliated with Hamas. Article 20 specifically targets the propagation of news that threaten state "national unity", "national security" and "public order". Palestinian activists argued the arrests were politically motivated, unsubstantiated and demanded the release of journalists, which led to sit-ins as well as social media campaigns such as #Journalism_Is_Not_a_Crime.

Human rights activists have also been targeted by law no. (16). On 4 September 2017, prominent human rights activist Issa Amro was arrested for advocating the release of an imprisoned journalist who mocked President Abbas. Consequently, a coalition of 11 civil society organizations formed a legal commission and submitted a memo to Hanan Ashrawi, the head of the Palestinian Liberation Organization's department of culture and information, with detailed objections to the law's provisions.[6] Following this civil society backlash, the Palestinian Ministry of Justice organized dialogue sessions, which many considered long overdue, with civil society organizations to present and discuss amendments to the cybercrime law no. (16).

Due to pressure from the coalition, amended cybercrime legislation, law no. (10), was published on 3 May 2018 to replace law no. (16).[7] The coalition succeeded in pushing for the removal of Article 20 as well as the reduction of harsh penalties, the omission of criminalization related to loosely defined terms such as national unity and the public order as well as the addition of new provisions such as Article

21 of law no. (10) that protects media, publication and artistic freedoms. But despite these amendments, several other concerns, highlighted in the original version law no. (16), related to excessive powers, and illegal collection of evidence remained unchanged in the 2018 law. Additionally, Article 40 in law no. (16) granting power to block websites remained as Article 39 in law no. (10). Organizations such as the Palestinian Independent Commission for Human Rights and 7amleh maintained that several problematic provisions in violation of Palestine's international obligations remained. Nonetheless, the new draft was issued and published in the official gazette in May 2018 without having undergone adequate consultation.

The original cybercrime law no. (16) ultimately added to restrictions on Palestinian media and press freedoms imposed by Israeli security forces, such as constant raids of media centers and the political detention of journalists, contributing to a pre-existing environment of fear and mass surveillance. It equips Palestinian security forces with a legal mechanism to limit access to information and arbitrarily detain journalists and activists. In fact, a report by the Palestinian Centre for Development and Media Freedoms shows that the number of violations of media freedoms committed by Palestinian security forces in June 2017 were higher than those committed by Israeli occupation forces, peaking after law no. (16) enactment.[8] The use of law no. (16) to crack down on civil dissent and freedom of expression raises further concern because of its impact on the prospects for positive sustainable change which highly relies on the openness of Palestinian society and trust in their leadership, mainly in the socio-economic and political spheres in Palestine. Both have been shaken by this crackdown on civil liberties and freedom of expression.

Secretive legislation in the context of a legitimacy crisis

Considering its social and political implications, the original cybercrimes law no. (16) is part and parcel of the PA's securitocratic approach, when a regime relies on its security apparatuses and institutions to consolidate its rule, faced with a legitimacy crisis and increased civil society discontent with a stagnant status quo.

Over the past decade, dissatisfaction with the leadership's efforts to end the occupation and to provide for and govern its citizens has increased.

A 2017 poll by the Palestinian Center for Policy and Survey Research reported that two thirds of Palestinians want Abbas to resign, having ruled for 11 years exclusively by presidential decree.[9] According to civil society activists, the new law is an attempt to consolidate a government that is losing legitimacy in the eyes of its people, by creating fear of censorship and detention rather than building a protective environment based on trust. But the use of the cybercrimes law to control the digital sphere, one of the only platforms for free political expression in Palestine, is problematic as it leads to self-censorship, stifles the potential for grassroot change and necessary discussions about Palestinian leadership.

Furthermore, the Palestinian Legislative Council (PLC) has been inactive since the failure to form a government after the 2007 elections. In turn, this has led to a concentration of excessive legislative and judicial powers in the hands of the executive. Under Palestine's Basic Law, legislation can be issued by presidential decree in cases of necessity. However, considering the continuation of Palestinian divisions and inability to revive the PLC, legislation by decree has been the norm since 2007 and cybercrime legislation is only one among hundreds of decrees. This predicament makes it critically important for the executive branch of government to practice these powers in a transparent and consultative manner. The environment of increasing distrust and dissatisfaction with the PA's rule accompanied by the President's unilateral efforts to enact such legislation raises larger questions about the accountability of the Palestinian government.

Law no. (16) impact on political plurality

Considering Palestine's environment of continued political infighting, law no. (16) has also had implications on political plurality in Palestinian society. It has contributed to deepening political rivalries as it was used to silence political opposition to Abbas's presidency coming from Hamas and Dahlan affiliates. Article 40 of the cybercrime law no. (16) allows police and security forces to request the Attorney General to shut down and block access to websites that publish content that threatens "public order" or "public peace" within 24 hours. Under such loose

definitions, the authorities have the power to block websites that do not promote their interests or a certain political agenda. Twenty-nine news and media outlets affiliated to the political opposition as well as other independent media outlets critical of the PA leadership were shut down using Article 40. The new version of the cybercrime law no. (10) issued in 2018 still includes this provision.

Hamas deputies have spoken out against the 2017 law, due to what they see as an illegitimate legislative process that only advances the West Bank's PA's narrow interests. However, this is not to say that Hamas has not played a similar role silencing internal opposition. An Amnesty International report on the state of freedom of expression in Palestine states that both governments have been using "police state tactics", and that the Hamas security forces have also arrested 12 activists and journalists who expressed opposition on social media in June 2017.[10] Such moves to silence and censor dissent and free expression contradict democratic principles and contribute to consolidating what many Palestinians see as an illegitimate rule. Moreover, Palestinian political division has for long stood as a key obstacle to the peace process, state-building, and an end to the 70-year long Israeli military occupation.

Challenges and conclusions: A cybercrime law without a cybersecurity strategy

Faced with the increasing threat of cybercrime, enacting new legislation should not be a standalone effort but part of a comprehensive cybersecurity strategy. According to the International Telecommunications Union (ITU) 2014 cyber wellness, Palestine lags on the technical, legal, organizational, capacity building and cooperation levels. It has no official standards to oversee the implementation of international cybersecurity standards and conventions; it has no framework in place to measure national cybersecurity development, it did not have, until recently, a Computer Emergency Response Team nor are there official frameworks in place for regional, international and public sector cooperation.[11] According to an ITU study, protective cybersecurity measures must be comprehensive and taken within the five pillars of the Global Cybersecurity Agenda, which include

capacity building, legal measures and international cooperation. Hence, to develop an adequate response to cyber vulnerability in Palestine, cyber awareness and a cyber culture needs to be institutionalized by service providers and users, and cooperation needs to be strengthened between public and private sectors in a transparent and engaging way.

Considering the government's move to provide citizen welfare through e-services, digitizing all kinds of citizen data and with the ICT industry contributing around 10% to the Palestinian economy, a cybersecurity strategy should protect the interests of users, businesses and the government alike, and developing a criminal legislation is part of it. This pertains to the importance of developing legislation through a consultative process, maintaining principles of transparency and accountability. However, as the original piece of legislation was developed in secrecy, this calls into question its protective capacity, but also the leadership's accountability and institutional transparency. Institutional challenges such as the inactiveness of the PLC hinder the legislative process and institutional ability to combat crime. However, the government remains accountable to inform and consult with civil society coalitions before activating new pieces of legislation.

A positive aspect is that Palestinian grassroot mobilization and activism against such policies offers a glimpse of hope that the slide to authoritarianism will not go unchallenged. In a system void of checks and balances, civil society plays a key role in unveiling and denouncing unconstitutional and repressive governmental measures and must be encouraged. Palestinian CSOs defended their right to peaceful criticism of the government and made use of digital platforms and media advocacy tools to increase organizational and communal awareness of key concepts such as digital security. To this end, organizations such as 7amleh, The Arab Centre for Advancement of Social Media, have led efforts to engage and sensitize citizens of developments affecting their digital rights.

Finally, the cybersecurity capacity in Palestine has been impacted by the Israeli government's control of Palestinian ICT infrastructure, ICT imports, and telecommunication frequencies. While there is a clear need to increase Palestine's cybersecurity prevention capacity, this must be carried out in compliance with the PA's international obligations regarding individual privacy and freedoms, and refrain from infringing on political activity that contribute to the necessary

democratization and openness of Palestinian society.

Endnotes

1. Abdelbaqi, Mustafa, Global Journal of comparative law, "Enacting Cybercrime Legislation in an Endeavour to Counter Cybercrime in Palestine", 30 July 2016.

2. Donia Al Watan, "Palestinian Women increasingly targeted online", 31 January 2016, english.alwatanvoice.com

3. To access to the original text of the law, see: 7amleh, "The Full English Translation of the Palestinian Cybercrime Law", 02 August 2017, 7amleh.org

4. The Guardian, "'Any Palestinian is exposed to monitoring by the Israeli Big Brother'", 12 September 2014, available at: theguardian.com

5. For more on Israeli legislation and its impact on digital freedoms, see: 7amleh, " Will a new wave of Israeli legislation diminish internet freedoms?", 14 August 2018, 7amleh.org

7. To access the new cybercrime law no. (10), see: Palestinian News and Info Agency, "Legislation by decree no (10) of 2018 on Cybercirme", 03 May 2018, available at: wafainfo.ps

8. MADA, "MADA: 51 violations of media freedoms in Palestine during June 2017", madacenter.org, accessed [August 2018]

9. PCPSR, "Public Opinion Poll No (63)", 26 March 2017, available at: pcpsr.org

10. Amnesty International, "Palestine: Dangerous escalation in attacks on freedom of expression", 23 August 2017, available at: amnesty.org

11. ITU, "Cyberwellness Profile State of Palestine", itu.int, accessed [November 2017]

Arab Reform Initiative

About the author

Chiara Ayad

Chiara Ayad is a project coordinator at the Norwegian Center for Conflict Resolution. Until July 2019, she was a Researcher and Programme Officer at ARI, in charge of coordinating the project on Decentralization as well as research on Gender dynamics in radicalization and Countering Violent Extremism (CVE). She holds a Master's degree in International Security from Sciences Po Paris, the Paris School of International Affairs (PSIA) and an undergraduate degree in Middle Eastern Studies from Sciences Po Menton and the School of Oriental and African Studies (SOAS), University of London.

About Arab Reform Initiative

The Arab Reform Initiative is the leading independent Arab think tank working with expert partners in the Middle East and North Africa and beyond to articulate a home-grown agenda for democratic change. It conducts research and policy analysis and provides a platform for inspirational voices based on the principles of diversity, impartiality and social justice.

- We produce original research informed by local experiences and partner with institutions to achieve impact across the Arab world and globally
- We empower individuals and institutions to develop their own concept of policy solutions
- We mobilize stakeholders to build coalitions for positive change

Our aim is to see vibrant democratic societies emerge and grow in the region.

Founded in 2005, the Arab Reform Initiative is governed by a Plenary of its members and an Executive Committee.

arab-reform.net

contact@arab-reform.net

© 2018 by the Arab Reform Initiative.
To view a copy of this licence, click here